REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	10.Aug.04	DISSERTATION

4. TITLE AND SUBTITLE
PROTECTING STATE AND LOCAL CRITICAL INFRASTRUCTURES: WEAVING TECHNOLOGY, LEGISLATION AND POLICY

5. FUNDING NUMBERS

6. AUTHOR(S)
COL ARATA HAROLD J III

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
UNIVERSITY OF TULSA

8. PERFORMING ORGANIZATION REPORT NUMBER
CI04-577

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
THE DEPARTMENT OF THE AIR FORCE
AFIT/CIA, BLDG 125
2950 P STREET
WPAFB OH 45433

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited distribution
In Accordance With AFI 35-205/AFIT Sup 1

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS	15. NUMBER OF PAGES
	133
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government

Abstract

Harold J. Arata III (Ph.D. in Computer Science)

Protecting State and Local Critical Infrastructures: Weaving Technology, Legislation and Policy (133 pp. – 11 Chapters)

Directed by Professor Sujeet Shenoi

(147 words)

State and local governments rely on critical infrastructures to provide vital services to citizens. Furthermore, the majority of America's critical infrastructure components are physically situated in state and local jurisdictions. Still, the importance of state and local governments in national critical infrastructure protection efforts has been largely overlooked.

This dissertation focuses on strategies for engaging state and local governments in critical infrastructure protection and, in particular, helping secure electronic infrastructure components. State and local entities must be linked to federal and private sector programs, thereby implementing a new breed of federalism. Furthermore, state and local governments must participate in regional partnerships, expand education and training programs, and improve information sharing through state and local ISACs. Only by aligning and weaving the "threads" of technology, legislation and policy can state and local governments strengthen the fabric of their critical infrastructures and protect them from internal and external threats.

THE UNIVERSITY OF TULSA
THE GRADUATE SCHOOL

PROTECTING STATE AND LOCAL CRITICAL INFRASTRUCTURES: WEAVING TECHNOLOGY, LEGISLATION AND POLICY

by
Harold Joseph Arata III

A dissertation submitted in partial fulfillment of
the requirements for the degree of Ph.D.
in the Discipline of Computer Science
The Graduate School
The University of Tulsa
2004

Acknowledgements

I would like to express my gratitude to my committee members Dr. Shenoi, Dr. Hale, Dr. Papa, Dr. Donaldson and Dr. Buckley.

I would specifically like to thank my advisor, Dr. Sujeet Shenoi for his guidance, support and patience during my stay at Tulsa and over the course of different research activities. Also, I would like to thank Dr. Donaldson for being a gentleman and mentor, Dr. Buckley for the warmth he has shown me, Dr. Hale for all the office time he so generously gave up for me every time I asked, "Do you have two minutes," Dr. Papa for his smile which kept me going, Dr. Steib for his constant friendship and advice, Dean Belsky for his superb classroom instruction, guidance and support, Dr. Wainwright for his continual care and encouragement and Dr. Marks for the review time he gave.

Table of Contents

List of Figures

CHAPTER I

INTRODUCTION

Eighty-five percent of America's critical infrastructures and key electronic assets are owned and operated by the private sector. Because private sector critical infrastructures reside within states and local communities, state and local governments naturally must play a crucial role in their protection. Without state and local governments, the tasks of coordinating and integrating critical infrastructure protection across all levels of government and society would be virtually impossible to accomplish [70]. However, only two pages of the fifty-eight page White House *National Strategy to Secure Cyberspace* address state and local government concerns.

With so little written on state and local governments some might brand critical infrastructure protection a federal responsibility. But nothing can be further from the truth. States and local governments play a vital role in critical infrastructure protection. Indeed, the closest relationship the average citizen has with government is at the state and local level.

State and local agencies have primary responsibility for funding, preparing and operating the emergency services that would respond in the event of a natural disaster or terrorist attack. Moreover, many functions reserved for states within the nation's federalist system (e.g., supporting law enforcement efforts, maintaining medical records

and making welfare payments) require computer networks. Clearly if state and local electronic infrastructures fail, the consequences will be severe.

The task of critical infrastructure protection is inherently difficult and often overwhelming. It is therefore necessary to employ a defense in depth strategy to protect the information systems of state and local governments. Defense in depth can be realized by weaving technology, legislation and policy to establish a multi-layer, mutually supportive protection system—much like the metaphorical walls, moat, and interior chambers that make up the defenses of a castle.

The remainder of this dissertation is organized as follows:

Chapter II defines federalism and the vital role of state and local governments. Chapter III introduces critical infrastructures, describes the individual critical infrastructure components of the private and public sectors and clarifies their complex interdependencies. Chapter IV describes the vulnerabilities, threats and risks to America's critical infrastructures.

Chapters V through VII define the defense in depth concept by highlighting the roles of technology, legislation and policy, respectively. Specifically, Chapter V defines the technological element, which is comprised of enterprise security management measures, hardware controls, software controls, physical controls and human security controls. Chapter VI presents the legislative element, which is comprised of federal and state statutes that center on legislation such as the *Computer Fraud and Abuse Act*, the *Electronic Communications Privacy Act* and the *USA PATRIOT Act*. Chapter VII

presents the policy element, which articulates what must be protected, how resources are to be used and what must be done.

Chapter VIII highlights critical workforce and information sharing issues. Chapter IX recommends measures to be adopted by state and local governments to protect their critical infrastructures. Chapter X defines the distribution of responsibilities for costs and duties among federal, state and local levels of government; and ends by exploring the economic justifications for government intervention to protect state and local critical infrastructures. Chapter XI contains concluding remarks and recommendations for future work.

CHAPTER II

FEDERALIST CONSTRUCT—VITAL ROLE OF STATE AND LOCAL GOVERNMENT

Federalism is a system of government in which powers and responsibilities are divided between a national government and provincial or state governments [25]. The United States has a federal system of government that requires the national and state governments to work together on many critical issues, including critical infrastructure protection. Although matters of national security are handled solely by the federal government, the role and importance of states must not be overlooked in the critical infrastructure arena.

2.1 History of Federalism

In the days and weeks following the September 11 attacks, the mass media, and to some extent, the American public, seemed to conclude that the federal government would be forced to assume a new level of power to protect the American homeland, and "that terrorism would, and perhaps should, kill federalism" [42].

Yet many observers [43, 49] have asserted that the federalist construct of the United States will be of supreme importance to the nation's survival in the face of terrorist attacks and that it will continue to play an essential part in guiding the nation's future. Some scholars [43, 49] have asserted that (i) the federal system responded remarkably

well to the horrific events of September 11; (ii) the responses of local officials, as well as the civic and heroic behavior of citizens, vindicated the values of local self-government in a federal democracy; and (iii) counterterrorism, especially with respect to critical infrastructure protection, might require more, not less, federalism. Although the establishment of a new federal department may seem to brand homeland security a responsibility of the federal government, it would be incorrect to assume that state and local governments possess anything short of critical roles in preparing for and responding to terrorist attacks on American soil.

In the event of a terrorist attack, a great deal of the effort of attending to public health and safety must, by geographic and governmental necessity, transpire outside the Beltway. Although federal planners may possess the analytic capabilities to identify threats from foreign and domestic terrorist actors, and be able to assist in implementing appropriate security measures, much will ultimately be determined by the skill and performance of local authorities. In a vast country—with 3,718,000 square miles of territory, 12,373 miles of coastline, and at least 75 major population centers—potential terrorist targets are numerous and widespread [6]. According to P. Nivola, an expert on federalism, "to the extent that government bureaucracies have the ability to prepare communities for the worst eventualities, and can respond effectively in an emergency, the responsibility will rest in large part with local agencies that are closest, so to speak, to the facts on the ground" [58].

Nevertheless, homeland security is among the primary responsibilities of government at all levels. The President and the federal government will be called upon for guidance in the way of national policy recommendations such as the *National*

Strategy to Secure Cyberspace [6] and through financial commitments. State and local governments will be expected to implement numerous programs and provide services directly to the American populace. Yet as history has shown, the balance of power between the levels of government in the United States is delicate. Not all matters may be easily divided between the federal government and the states. A clean and stable demarcation between federal and local roles has proven impossible to draw over time. But by no means should this difficulty be allowed to drive one to futility, nor to force one to "the proposition that the concerns of national and local authorities can only be randomly distributed" [58]. Instead, as the United States confronts its first major challenge of the twenty-first century, it is important to once again reevaluate this enduring tension in the structure of American government. Among the many basic questions surrounding policy for homeland security lies the difficulty inherent in a federalist government: What are the proper spheres of national and local jurisdiction?

Supreme Court justices, scholars of federalism and reflective citizens have grappled with this issue since the country's inception. At the height of the Cold War, when many were fearful that Russian nuclear warheads were pointed at American cities, President Eisenhower directed the Commission on Intergovernmental Relations to prepare an emergency response plan for use in case of a disaster and to demarcate a sensible separation of duties among levels of government. The results were far from unconventional, as the report seemed to be yet another dose of Washingtonian groupthink. The staff report that was released, "*Civil Defense and Urban Vulnerability*," concluded that "intergovernmental responsibilities were inappropriately defined and

assigned, and then turned around to make such recommendations as more national financial assistance to states and cities" [11].

The challenge at this time is to avoid this trap and instead develop an approach to homeland security and critical infrastructure protection in which policy issues are addressed by the appropriate levels of government. Before one may move toward such an approach, though, it may be helpful to briefly survey the history of federalism in the United States, for as Sir Winston Churchill put it, "the farther backward you can look, the farther forward you are likely to see."

The complex history of U.S. federalism has been the subject of numerous scholarly works, and the many trends and particularities could be explored *ad infinitum*. Since this work is not a dissertation on American federalism, only a basic historical account of American federalism is provided. With this said, U.S. federalism may be broken into five major eras [44]: (i) pre-1789, national supremacy supported by early efforts to establish the legitimacy of the new nation; (ii) 1789-1901, state-dominant dual federalism based on the shared presumption that the states and their localities had sufficient regulatory and fiscal power to meet the nation's modest domestic demands except in well-defined and limited circumstances; (iii) 1901-1960, Washington-dominant cooperative federalism from the New Deal through World War II in response to the national crises of a global depression and two World Wars; (iv) 1960-1968, creative federalism beginning with President Johnson's Great Society plan as a result of the Korean War and the Cold War which reinforced the permanency of the shift from state—to Washington—dominant federalism; and (v) 1970 to present, the "new federalism" of the remaining part of the

20th century which saw a significant devolution of national programs and an increased support for state's rights [44].

2.2 National Crises and the Concentration of National Power

Wars and national crises tend to strengthen and extend the arm of federal power. Following the Civil War, diversity among states was no longer seen as a source of liberty. While individual states may have spearheaded progressive reforms, only the national government had the ability to take that agenda to all states. The national government became a more active regulator and reformer in the economic system, while state reforms focused on traditional areas of law enforcement and services such as hospitals, sanitation and public welfare.

After a period of relative peace and stability in which states regained a great deal of authority, the nation was swept into World War I and then into the Great Depression in the 1930s. Again, in response to a national crisis, the federal government experienced a remarkable growth in power. Alexander Hamilton argued in the *Federalist Papers* that a strong national government was needed to protect the Union from its enemies and to ensure the stability and livelihood of commerce [31]. According to K. Ladenheim [44], "[Hamilton's] theory was vindicated as a global depression and two World Wars led to the most powerful national government in the history of the United States" [44]. The federal government replaced the constraints created by the time-honored but narrow interpretation of its constitutional powers with the New Deal, an empowering formula based on a very broad interpretation of federal constitutional power. This period saw explosive growth in the national government and the relative contraction of both the

private and state/local sectors' shares of the economy. J. Shannon has emphasized that the badly shaken middle-class, "radicalized by unprecedented unemployment, mass foreclosures of homes and farms, and widespread bank failures, turned to the national government for extraordinary help" [77].

The national government played such a dominant role in the New Deal and World War II that some students of federalism had declared an end to federalism as the founders intended. They were incorrect in their assertions, however. Although President Johnson's Great Society seemed only to confirm federal supremacy, the next twenty-five years saw a marked resurgence in state autonomy and continued fiscal devolution from the federal to the state level. Much in the same way that national crises tend to concentrate power at the national level, the lack of crises tends to push some of that power back to the states. The absence of wars and national emergencies often spawns a resurgence in state authority. The recent federalism revival should not come as a surprise, then, as the post-Cold War atmosphere of tranquility allowed many states to pay less attention to the federal government.

In the eyes of many scholars, the latest push for states' rights, culminated in the landmark 1995 Supreme Court decision *United States v. Lopez*. This case invalidated the federal *Gun Free School Zones Act* which prohibited the possession of guns in and around schools [78]. Recently, the Supreme Court has shown signs of defining and separating areas of state and national authority. In the *Lopez* case, in particular, the Court decided that the national government had reached into what should be state police powers in the matter of guns near schools.

But, in the spirit of contradictory decisions from the Supreme Court, the *Lopez* case may be directly contrasted to the 1985 *Garcia* decision which effectively overturned the Tenth Amendment in favor of states' lobbying Congress. In addition to carving out specific matters of state authority, the current era in the history of federalism has also been marked by a flood of rulings in favor of sweeping federal powers. For example, the federal penal code has expanded to include so many offenses in the last decade that the American public, including judges and even lawmakers, have become confounded. "We federalize everything that walks, talks, and moves," Senator Joseph Biden of Delaware has complained [58]. Writing about this massive growth in federal law, Chief Justice William Rehnquist stated that "the pressure in Congress to appear responsive to every highly publicized societal ill or sensational crime needs to be balanced with an inquiry into whether states are doing an adequate job in these particular areas" [58]. Ultimately, he said, Congress and the nation must choose "whether we want most of our legal relationships decided at the national rather than local level" [58]. Rehnquist's words resonated with many skeptics. University of Texas law professor Ernest Young stated, "Particularly today, chasing car thieves, medicinal marijuana users, unwitting wetlands trespassers, and deadbeat dads does not seem like the best way for federal law enforcement to spend its time" [111].

2.3 Areas of National Responsibility

Yet even those most skeptical of modern federal power acknowledge important areas of national responsibility. Most would agree that the federal government rightfully bears the responsibility for several areas, including securing the nation against foreign threats, investigating multi-state criminal conspiracies, ensuring the safety of the nation's

air transport system, patrolling borders and gathering intelligence about terrorist organizations. In these traditional areas of national power, particularly those relevant to the United States' war against terrorism, many scholars have expressed their beliefs that nothing in the Supreme Court's effort to revive constitutional limits on federal power will stand in the way of the President and Congress.

This effort has generally been limited to decisions which have invalidated federal laws where no plausible justification for national action exists (e.g., *Lopez*). Moreover, the Court has simultaneously reaffirmed broad federal power to address problems of national scope. There is little doubt, for example, that the Rehnquist Court would unanimously uphold a federal law nationalizing airport security, or expanding the investigatory powers of the FBI, if such a law were challenged on the basis that it was the exclusive province of the states. And although the Court's 1997 decision in *Printz v. United* States[1] might limit the Secretary of the Department of Homeland Security's ability to compel state and local law enforcement to participate in counterterrorism operations, "does anyone doubt that state and local officials will jump at any chance to cooperate with federal security efforts?" [111].

---

[1] Jay Printz v. United States centered on whether certain interim provisions of the Brady Handgun Violence Prevention Act violated the Constitution. The Brady Act amended a detailed federal scheme that governed distribution of firearms established by the Gun Control Act of 1968. Interim provisions directed state law enforcement officers to participate in administration of a federally enacted regulatory scheme. Petitioners, chief law enforcement officials (CLEO) of their respective counties, objected to being pressed into federal service and contended that congressional action that compelled state officers to execute federal laws was unconstitutional. The Supreme Court agreed and held that the interim provisions violated constitutional principals of dual sovereignty and separation of powers. Congress cannot compel states to enact or enforce a federal regulatory program. Congress cannot circumvent that prohibition by conscripting the state's officers directly. The Brady Act effectively transferred the executive branch's responsibility to administer federal laws to thousands of CLEOs in 50 states, who were left to implement the program without meaningful presidential control [58].

Regardless, there has been much talk suggesting that the Supreme Court's pre-September 11 efforts to reinvigorate the Constitution's limits on national power are now out of step with current imperatives. Linda Greenhouse, for example, recently wrote that "the era of states' rights decisions, a luxury of tranquil times, now seems like a vestige of bygone era" [30]. Although it would be incorrect to proclaim the death of federalism as some scholars did in response to the New Deal, Greenhouse is among many observers who believe that the nation will soon find itself in a new period of Washington-dominated federalism. Recalling the historical wave of federalism as previously discussed, it seems apparent that whenever a national emergency occurs, the concept of federalism disappears. Robert C. Post, a law professor at Yale University, has explained that "in a national emergency, you give the national government the power to get done what needs to get done" [30]. Given this propensity to concentrate power at the national level in times of crises, it is important not to lose sight of the structure of government the founding fathers established. One must remember that "the autonomy of the states and the idea of limited national power are no less important bulwarks of individual liberty than the more familiar provisions of the Bill of Rights" [111].

The framers of the Constitution originally believed a Bill of Rights was unnecessary to protect freedom, provided that the Constitution's structure limited the authority of the federal government. Although history has since demonstrated the importance of specific provisions for particular rights, "nothing in our experience suggests that the original safeguards of federalism and separation of powers have become irrelevant or obsolete" [111].

In arguing for the creation of a federal rather than unitary system, Alexander Hamilton stated: "An entire consolidation of the States into one complete national sovereignty would imply an entire subordination of the parts and whatever powers might remain in them would be altogether dependent on the general will. But as the plan of the [constitutional] convention aims only at a partial union or consolidation, the State governments would clearly retain all the rights of sovereignty which they before had, and which were not, by that act, exclusively delegated to the United States" [32].

2.4 Renewed Importance of State and Local Governments

Former Michigan Governor and former chairman of the National Governors' Association, John Engler, believes that "the Founding Fathers had it right" [111]. The founding fathers assigned multiple and enumerated powers to the federal government and reserved the others for the states. Engler believes, as seen from the tragedy of September 11, that Congress needs to be focused on international issues, on issues of foreign affairs and intelligence gathering and in operating the nation's military [111]. State and local governments, Engler insists, are capable of managing the rest of the responsibilities. Although these comments are clearly from a states' rights proponent, they do seem to resonate with the words of Hamilton.

While government response to the 9/11 attacks clearly demonstrated the importance of federal power, they also reaffirmed the importance of the state and local governments that the Supreme Court's decisions have sought to protect. In a federal system, state and local governments have sovereign responsibilities (e.g., law enforcement and emergency services) and are the first line of homeland defense. The rescue workers who responded

with valor and sacrifice at the World Trade Center were overwhelmingly officers of state and local governments. The National Guardsmen patrolling the nation's airports and responding to emergencies continue to serve the states in order to protect lives and property. Citizens will continue to depend on state and local law enforcement to provide the first—and often only—line of defense against future terrorist attacks.

With the federal agenda and budget increasingly focused on terrorism and law enforcement issues that surround it, it is at the state and local level where homeland security and the protection of critical infrastructures will actually be implemented. As Washington focuses on prosecuting the war against terrorism, citizens must increasingly rely on state and local governments to provide a variety of low profile but critically important services, from law enforcement to emergency response.

CHAPTER III

CRITICAL INFRASTRUCTURES

The protection of critical infrastructures is a shared responsibility. Federal, state, local and private sector entities rely extensively on computerized systems and electronic data to support their operations. Critical infrastructure protection involves activities that enhance the security of cyber and physical infrastructures essential to the nation's security, economic viability, and public health and safety. Because eighty-five percent of the nation's critical infrastructures are owned and operated by private sector entities [85], collaborative efforts between the public and private sectors are necessary to avoid disruptions in critical operations, data tampering and the inappropriate disclosure of sensitive information. This chapter focuses on critical infrastructures, describes the individual critical infrastructure components of the private and public sectors and closes by examining their complex interdependencies.

3.1 Overview

Critical infrastructures are "those physical and cyber-based systems essential to the minimum operations of the economy and government" [52]. More specifically, critical infrastructures are essential systems for telecommunications, electrical power, gas and oil storage, banking and finance, transportation, water supply, emergency services and continuity of government operations. The *USA Patriot Act* defines critical infrastructures as "systems and assets, whether physical or virtual, so vital to the United States that the

incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [19]. When members of the public flip on light switches, they expect light. When they pick up telephones, they expect dial tone and service. When they turn on taps, they expect running water. At a hospital, they expect hospitals to operate and medical care to always be available [85]. All of these services rely on the proper functioning of critical infrastructures.

When critical infrastructures fail, the consequences can be severe. The lack of electrical power, telecommunications services, running water and hospital services during an emergency could cause mass chaos. In fact, if physical attacks were accompanied by attacks on the nation's critical infrastructures, hundreds or thousands of lives could be lost. Ronald Dick, former director of the FBI's National Infrastructure Protection Center, stated that the events he fears most are "physical attacks in conjunction with a successful cyber-attack on the responders' 911 system or on the power grid that supports them" [26]. These additions to a conventional attack might mean "first responders couldn't get there, water didn't flow and that hospitals didn't have power. Is that an unreasonable scenario? Not in this world. And that keeps me awake at night" [26]. In fact, in 1996, a man sitting in front of a computer at his home in Goteburg, Sweden, disabled most of southern Florida's 911 emergency response systems [15].

3.2 Critical Infrastructure Sectors

The nation's critical infrastructures have been organized by the federal government to mirror each of the major sectors of the economy. President Clinton's 1998,

Presidential Decision Directives 63 (PDD 63), identified eight private sector infrastructures and five special functions. The original eight private sector infrastructures included [86]: (i) information and communication, (ii) banking and finance, (iii) water supply, (iv) transportation (e.g, aviation, highway, mass transit, pipelines, rail, waterborne commerce), (v) emergency law enforcement, (vi) emergency fire services and continuity of government, (vii) oil and gas production and storage, and electric power, and (viii) public health. In July 2002, several new sectors were introduced in President Bush's *National Strategy for Homeland Security*. The new sectors are: agriculture and food, chemical and hazardous materials, and postal and shipping [86]. Each will require coordinated security efforts on the part of federal, state and local governments, and the private sector.

3.3 Critical Infrastructure Special Functions

Certain critical infrastructure functions must be performed by the federal government. To handle these governmental responsibilities, five special function areas were defined [85]: (i) national defense, (ii) law enforcement and internal security, (iii) research and development, (iv) foreign affairs and (v) foreign intelligence. It is important to note that unlike the critical infrastructure sectors, the special functional areas have no private sector counterparts. For example, the intelligence community comprises agencies responsible for the collection and dissemination to policy makers of intelligence information on foreign threats. This critical role is unique to government and supports the Department of Homeland Security's threat advisory system [84]. Similarly, nowhere in the federal government is the reliance upon information technologies more apparent than in the special function area of the Department of Defense, whose goal is to ensure

that national and international infrastructure dependencies do not adversely affect its mission of national defense and global force projection [16].

In summary, the overlapping ownership of assets and services within the nation's critical infrastructure sectors and special functions presents significant protection challenges. To better understand these relationships, the next section examines the individual critical infrastructure components of both the public and private sectors.

3.4 Public Sector Components

Public sector critical infrastructure components are broadly divided into three levels: federal, state and local. Critical infrastructure components are described in their respective categories below.

3.4.1 Federal Government Components

The federal government alone has the capability to use military, intelligence and diplomatic assets to further its interests outside America's borders. Inside America's borders, the federal government uses immigration and naturalization personnel, border agents and customs officials, port and air terminal security, and law enforcement agents. Furthermore, federal agencies conduct critical research activities, coordinate protection planning and perform consequence management functions [85].

In 1998, President Clinton called upon the federal government to become the model for information systems security. His *Presidential Decision Directive 63 (PDD 63)* instructed every federal agency to develop critical infrastructure protection plans for all critical infrastructure sectors and special functions. In addition to PDD 63, current

statutory authority for the security of federal information systems rests in: the *Computer Security Act of 1987*, *Government Performance and Results Act of 1993*, *Paperwork Reduction Act of 1995*, *Clinger-Cohen Act of 1996, the Government Information and Security Reform Act of 2001, the Federal Information Security Management Act of 2002* and *Executive Order 13011* which directs the implementation of the above acts through a chief information officer. These vehicles help the federal government implement critical infrastructure protection across all sectors [29].

In addition to developing protection plans for all critical infrastructure sectors and special functions, the federal government owns and operates a subset of the nation's critical infrastructures. For example, the federal government owns significant railroad assets to move weapons systems. The federal government also owns significant storage and pipeline assets for oil and gas. The strategic petroleum reserve is currently planning to lease some of its 240 miles of pipeline to ExxonMobil for more than 25 million dollars [93]. The federal government also owns a number of national public health facilities such as the National Institutes of Health and the Walter Reed (Army) and Wilfred Hall (Air Force) medical complexes. In the financial sector, the federal government owns and operates the Federal Mint. In the shipping and postal sector, the U.S. Postal Service has numerous facilities and significant operations staffed by more than 749,000 federal postal workers [85]. Congress has also transferred airport security responsibilities to the federal government with the creation of the Transportation Security Administration.

In summary, the federal government, like the private sector, owns and operates many critical infrastructure components. Figure 3.1 presents the federal-level critical infrastructure components and the agencies that are responsible for them [85].

Agency	Federal Components
• DHS	• Information & Communications, Postal, Emergency Services, Continuity of Government, Aviation, Highways, Mass Transit, Pipelines, Water Commerce, Rail
• HHS	• Public Health Services
• Agriculture	• Agriculture, Meat and Poultry (other foods – HHS)
• EPA	• Water Supply, Chemical Industry, Hazmat
• Energy	• Electric Power/Oil and Gas Production & Storage
• Interior	• National Monuments and Icons
• Treasury	• Banking and Finance
• Justice/FBI	• Emergency/Internal Law Enforcement Services
• CIA	• Foreign Intelligence
• State	• Foreign Affairs

Figure 3.1: Federal Government Components.

3.4.2 State and Local Government Components

All of America's fifty states and 87,000 local jurisdictions have a vital role in critical infrastructure protection. It is at the local level where law enforcement, the National Guard and critical emergency services to protect communities occurs. Moreover, it is at the state and local level where citizens are prepared for emergencies and where the preponderance of private sector critical infrastructures resides [85].

Although there is overlap at all levels of government, state and local critical infrastructure responsibilities are unique. Every disruption or attack is a local challenge. Regardless of who owns, maintains or operates the affected infrastructure, each attack requires an immediate response by state and local agencies who must bear the initial load of consequence management before the incident escalates to the federal level [85].

Like their federal-level counterparts, state and local governments also own and operate a subset of the nation's critical infrastructure components. For example, state and local governments own and operate over 19,500 municipal sanitary sewer systems, including an estimated 800,000 miles of sewer pipelines [85]. There are approximately 80,000 dams across America, and the federal government is responsible for only about ten percent of them. The remaining critical dams belong primarily to state and local government agencies. Mass transit has always been a major purview of state and local governments. Most mass transit systems are owned and operated by state and local agencies. The majority of each state's urban workforce relies on state and local public transportation for both their daily needs and as a means of evacuation in the event of an emergency. For example, every year passengers take approximately 9.5 billion trips on public transit systems; this is more traffic than rail and air combined [85]. Finally, the National Guard is a unique asset that is under state control when not federalized, reporting directly to each state's governor.

Like the federal government, state and local level accountability for critical infrastructure protection has been appropriately designated. Figure 3.2 presents state and local level critical infrastructure components and the agencies that are responsible for them [85].

Typical State Agency	State and Local Components
• HHS	• Public Health Services
• Agriculture	• Agriculture
• EPA	• Water Supply, Chemical Industry – Hazardous Materials
• Energy	• Electric Power, Oil and Gas Production and Storage
• Finance/Education	• Information/Communications, Banking & Finance
• Transportation	• Aviation, Highways, Mass Transit, Pipelines, Rail, Waterborne Commerce
• Justice/Public Safety	• Law Enforcement Services, Emergency Services, Continuity of Government
• Governor/State	• Military (National Guard)

Figure 3.2: State and Local Government Components.

3.5 Private Sector Components

Approximately eighty-five percent of the nation's critical infrastructures and key assets are owned and operated by the private sector. Thus, a solid organizational scheme for effective engagement and interaction with the private sector at all levels is essential. Without the private sector, coordinating and integrating critical infrastructure protection across all levels of government and society would be virtually impossible [70].

The private sector has relied heavily on information technologies to remain competitive and viable. Manufacturers, banking and financial institutions, transportation providers and other critical infrastructure sectors have all seized upon and will continue to enhance their information networks enabling increased efficiency, cost reductions and new services. For example, industry now uses electronic networks to lower costs through just-in-time manufacturing [87]. Furthermore, all of the critical infrastructure sectors

have now interlinked their services through the use of telecommunications and information systems to support power and water supply, financial services, transportation and other critical services [70].

The systems and infrastructures owned and operated by the private sector are expansive. There are more than 100,000 miles of rail, 1.7 million miles of pipelines, 2,300 power plants, 255,000 oil and gas production sites, 56,000 chemical plants, 1,625,000 farms, 74,000 food processing plants, 4,900 registered hospitals and over 1.7 billion miles of telecommunications cable laid. Figure 3.3 summarizes the nation's private sector critical infrastructure components [85].

Major Areas	Private Sector Components
• Public Health	• 4,900 Registered Hospitals
• Agriculture	• 1,625,000 Farms, 74,000 Food Processing Plants
• Water, Chemical	• 56,000 Chemical Plants
• Energy	• 2,300 Power Plants, 255,000 Oil /Gas Production Sites
• Telecommunications	• 1.7 Billion Miles of Cable
• Banking and Finance	• 23,000 FDIC Insured Institutions
• Transportation	• 100,000 Miles of Rail, 1.7 Million Miles of Pipeline
• Commercial Assets	• 391 Skyscrapers
• Defense	• 200,000 Firms in 215 Distinct Industries

Figure 3.3: Private Sector Components.

3.6 Information Systems and Critical Infrastructures

The nation's security and economy is very dependent on information technology and the information infrastructure. Logistic and telecommunications networks directly

support all critical infrastructures. The reach of these networks is not limited to cyberspace. They also control physical infrastructures such as electrical grids, pipeline pumps, chemical production, air navigation and stock market operations [86]. It is therefore essential to understand what assets, systems and functions make up the information and telecommunications critical infrastructure.

The term "information and telecommunications sector" is commonly used, but difficult to define. President Bush's Commission on Critical Infrastructure Protection defined telecommunications infrastructures as: "the networks and systems that support the transmission and exchange of electronic communications among and between end-users, such as networked computers" [89].

Today, the information and telecommunications sector's voice, data and video services are provided to public and private users primarily through three networks: (i) the Public Switched Telephone Network (PSTN); (ii) the Internet; and (iii) private enterprise networks [85].

The PSTN is a complex and diverse network that provides switched circuits for telephone, data and leased point-to-point services. The PSTN network consists of more than 20,000 switches connected by billions of miles of fiber and copper cable. The backbone of the PSTN infrastructures includes cellular, microwave and satellite technologies, and gateways for mobile users [85].

The second major component of the critical information infrastructure is the Internet. The Internet is a global network consisting of a series of packet-switched networks operating under a common set of protocols. Public and private sector critical

infrastructures access the Internet via Internet service providers (ISPs). Internet service providers interconnect with the PSTN through switches and routers located within dial central offices [85]. Indeed, the explosion that has occurred in cyberspace has been one of the great phenomena of the 20th century.[2] Every minute, over five million e-mail messages are sent around the world. As of 2003, there were nearly 260 million users internationally with Internet access, and there will be over 765 million users by 2005 [82].

The third major component of the critical information infrastructure is enterprise networks. Enterprise networks support voice, data and video needs of large corporations. Enterprise networks are a combination of leased telecommunications lines, public switched telephone networks and Internet providers [85]. Enterprise networks are often referred to as Intranets.

The information and telecommunications sector is being transformed very rapidly. Indeed, it is predicted that within five years, the information and telecommunications sector will experience the convergence of voice, data and video PSTN networks into a single digital packet-based network called the next generation network (NGN) [24]. Figure 3.4 illustrates the convergence of the PSTN architecture to the next generation digital network, along with the convergence to wireless Internet devices and an expanding optical core [55].

---

[2] Moore's Law (every 18 months processing power doubles while cost holds constant) and Metcalfe's Law (the usefulness, or utility, of a network equals the square of the number of users) are redefining not only how business is done in cyberspace but also how societal boundaries are defined [1].

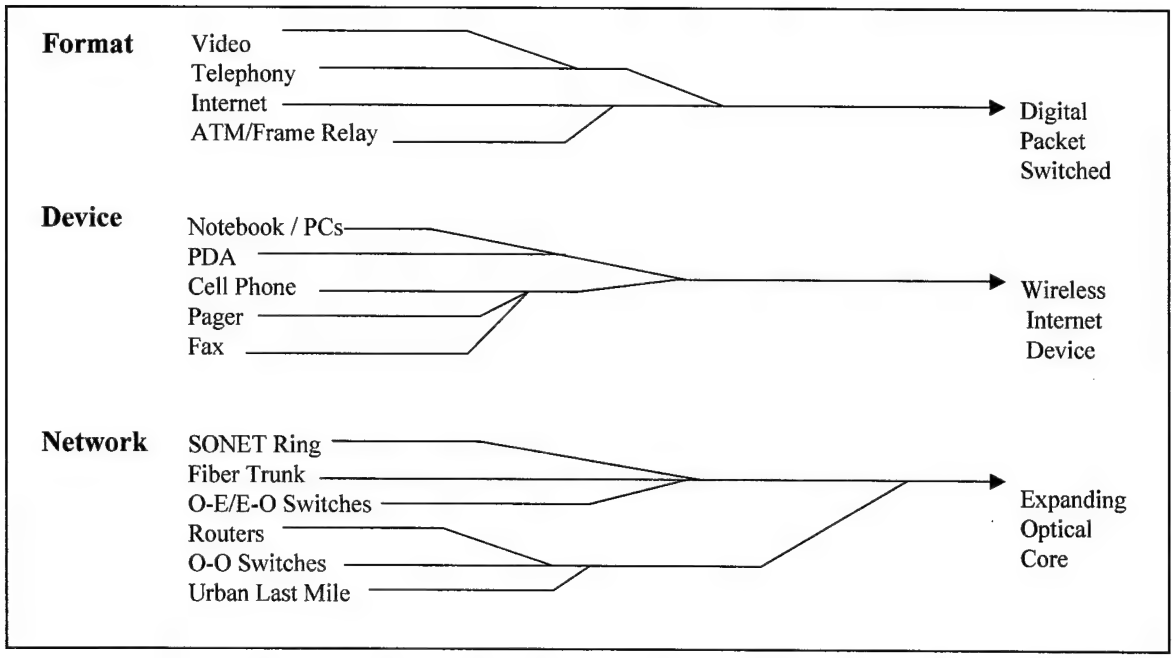

Figure 3.4: Critical Infrastructure Technology Convergences.

3.7 Critical Infrastructure Technologies and Protocols

To date, no comprehensive inventory of the information and telecommunications sector's assets has been published for either the public or private sector. However, the information and telecommunications sector does employ a vast array of technologies, standards and protocols. For example, signaling, control and management functions—ensure that power, water supplies, financial services, transportation and other critical services operate properly. Other types of control systems include Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are used primarily in industrial processes (e.g., steel making, power distribution, chemical production and in some experimental facilities). As such, SCADA systems are software packages that allow users to remotely control physical devices such as pumps and valves. SCADA

systems initially ran on DOS, VMS and UNIX; in recent years many SCADA vendors have moved to Windows NT and Linux [14].

New standards and protocols are being developed to secure information and telecommunications systems located within every critical infrastructure sector. Some of these new standards include: Internet Protocol version 6 (IPv6), which enables a variety of new features such as peer-to-peer and mobile applications; Voice over IP (VoIP), which enables sending voice information in digital form and in discrete packets rather than transmitting voice over the traditional circuit committed protocols of the public switched telephone network; Secure Border Gateway Protocol (S-BGP), which enables the authentication of IP addresses and enhances the security of communications between routers; and IP Security (IPsec) which enables secure, authenticated communications in operational systems.

3.8 Infrastructure Interdependencies

Interdependencies existing among critical infrastructures have long been recognized. In the 1930's, the Army Air Corps developed the industrial web theory which hypothesized that critical infrastructures were not only interconnected but that these interdependencies could be exploited by attacking key nodes, thereby disrupting the entire fabric of an enemy's economy [72]. Today's global economy is much more interconnected and interdependent than the industrialized nations of the 1930's.

Because of the growing interdependencies among the various critical infrastructure sectors, a direct or indirect attack on the information components of one sector could result in cascading failures across the others. Such interdependencies increase the need to

identify critical information assets and secure them against physical and cyber threats [85].

Virtually every infrastructure's key assets are monitored or controlled by networks and communication systems located within the information and telecommunications sector, creating inter-sector dependencies. One such interdependency exists between the information and telecommunications sector and the banking and finance sector. The banking and finance sector relies on computer networks and telecommunications systems to assure the availability of its services. The potential for disruption of banking and finance information systems is an important and special concern for this sector. For example, following the September 11 attacks, the equity securities market remained closed for five business days because telecommunications lines connecting key market participants were damaged [85]. In the transportation sector, nearly all flight navigation systems are interconnected and controlled by the information and telecommunications sector. The disruption of key navigation aids has caused entire airports to be closed until the information systems that support them could be secured. In order to control critical pumps and valves, the pipeline industry's remote monitoring and control systems (e.g., SCADA) rely heavily on the information and telecommunications sector being available and secure.

Indeed, all critical infrastructure sectors have become increasingly interconnected, software driven and remotely managed. The interdependencies of the other sectors with the information and telecommunications sector has become a double-edged sword. The information and telecommunications sector serves and enhances the operations of all the other sectors, while at the same time harboring the potential for massive disruptions and

cascading outages [37]. Because government and industry rely heavily on the information and telecommunications infrastructure for vital communications and control services, protection of this sector is particularly important [85].

The scenario, depicted in Figure 3.5 further illustrates these dependencies. In this example, within the information and telecommunications sector, a microwave tower that controls the SCADA systems for an electrical power grid is knocked offline. The disruption of SCADA monitoring and control causes a large generating unit to fail which in turn causes loss of power at a distribution station. This loss leads to blackouts in the region and increases the travel time for repair crews [66].

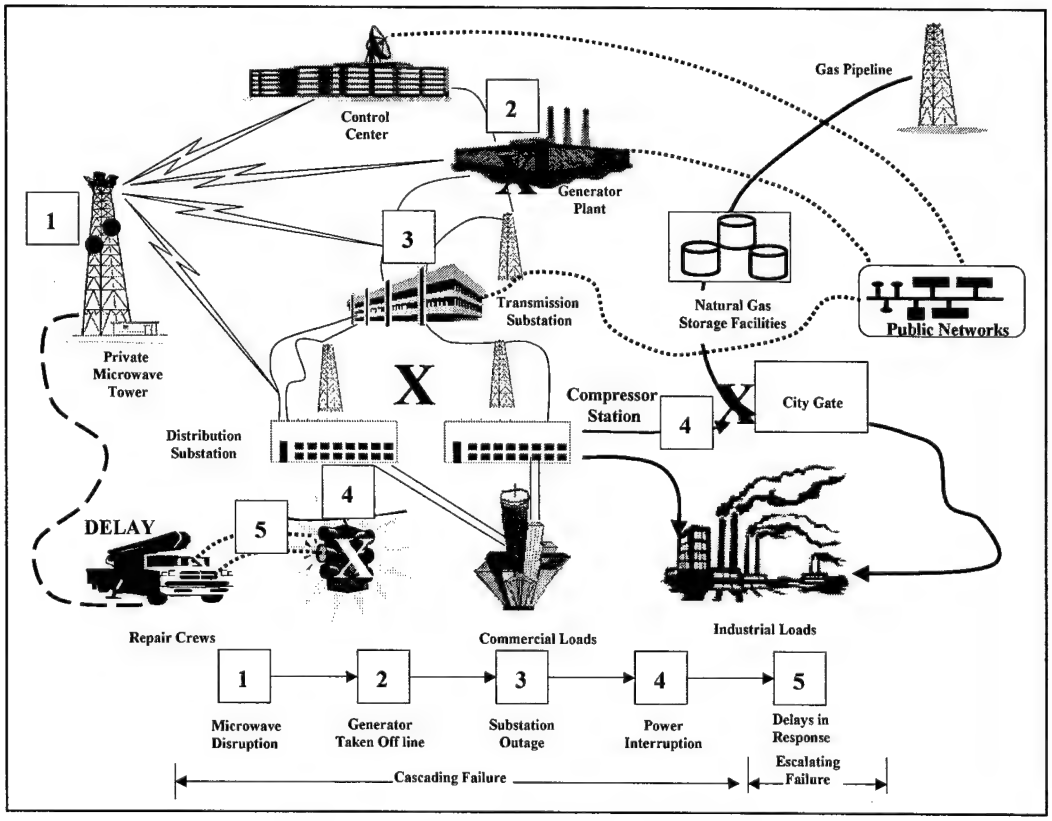

Figure 3.5: Interdependency Scenario.

The infrastructure interdependencies described in the previous scenario, can be divided in four main categories [66]:

1. **Physical**: Occurring when the material output of one infrastructure is used by another.
2. **Cyber**: Occurring when one or more infrastructures utilize electronic information and control systems.
3. **Geographic**: Occurring when infrastructures are situated in a common location.
4. **Logical**: Occurring when infrastructures are linked, e.g., through financial markets.

Traditionally, interdependencies are physical and geographic. However, because of the increased use of automated monitoring and control systems, along with the increased reliance on open markets for purchasing and selling commodities, there has been a shift in the prevalence and importance of cyber and logical interdependencies [66].

Physical, cyber, geographic and logical interdependencies go beyond individual infrastructure sectors and individual companies. Furthermore, they vary significantly in complexity from local linkages, which include municipal water supply systems and local emergency services, to regional linkages which include electric power coordinating councils, to national linkages which include interstate natural gas and transportation systems [66]. Figure 3.6 presents the infrastructure interdependencies from a "system of systems" perspective [108].

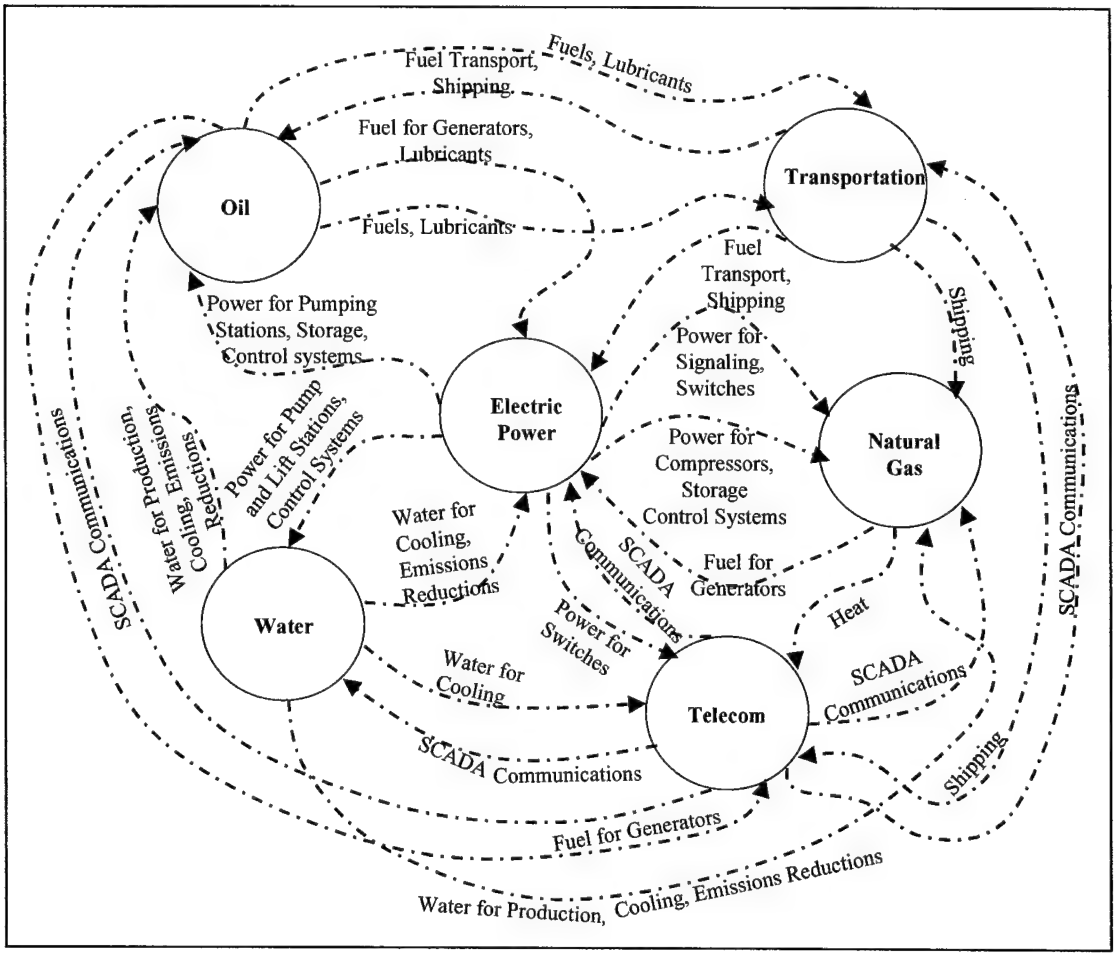

Figure 3.6: Infrastructure Interdependencies.

Critical infrastructures are true "systems of systems" and are interdependent. A failure in one sector or asset can cascade to produce disruptions or failures in others. The consequences of these failures could have devastating effects on the economy, public health and safety, national security and public confidence. Protection strategies must take into account these interdependencies in order to adequately protect critical infrastructures [85]. Indeed, the economic strength, profitability and viability of industry and the functioning of government are dependent on the reliability of these complex critical infrastructure networks [87].

No matter what technologies are involved or what sector they reside in, the national goal to protect critical infrastructures will continue to center around three primary objectives. The first is to ensure that the federal government performs essential national security functions. The second is for state and local governments to maintain order and deliver essential public services. The third is for the private sector to ensure the orderly functioning of the economy by delivering telecommunications, energy, financial, transportation and other services. By accomplishing these three goals, "any interruption or manipulation of these critical functions should be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States" [19].

CHAPTER IV

THREATS TO CRITICAL INFRASTRUCTURES

Cyber attacks on critical infrastructures can have tremendous consequences such as disrupting vital operations, causing loss of revenue and intellectual property, even loss of life. Countering such attacks requires the development of robust cyber security capabilities where they do not exist. Critical infrastructure sectors must continue to reduce their vulnerabilities, and identify and deter attacks. This section begins by evaluating vulnerabilities, threats and risks to America's critical infrastructures and ends by examining the various actors that could disable or disrupt America's core critical infrastructure functions.

4.1 Characteristics of Critical Infrastructure Computer System Attacks

Any part of a critical infrastructure computing system can be the target of an attack. A computing system is a collection of hardware, software, storage media, data and people [68]. All computing systems are susceptible to vulnerabilities and threats—producing risk—which can be potentially exploited by an attack.

4.1.1 Vulnerabilites

A vulnerability is a characteristic of a critical infrastructure's design, implementation or operation that renders it susceptible to compromise, disruption or destruction by a threat [74]. Common sources of vulnerabilities include security design flaws, social engineering, innovative misuses and incorrect implementation. For example, a computer system may be vulnerable to unauthorized data manipulation because the system does not satisfactorily verify user identity before permitting access [68]. Known vulnerabilities are the most common source for attacks and intrusions. Hackers write automated tools to exploit vulnerabilities within every critical infrastructure sector and system. In fact, many network intrusions require minimal technical expertise because vulnerabilities, technologies and attack tools for exploiting known vulnerabilities are often shared on the Internet.

Because the information infrastructure serves as a container and a transport medium for all other critical infrastructure sectors, its vulnerabilities impact all sectors. To reduce losses, enterprises must research and rank known vulnerabilities. One method of ranking vulnerabilities is through a qualitative measurement matrix. The definitive characteristic of the qualitative approach is the use of ordinal rankings, which include the following vulnerability categories [74]:

- **No Vulnerability**. A critical infrastructure, which by design, implementation or operation, has no assessable susceptibility to destruction or incapacitation by a threat.

- **Low Vulnerability**. A critical infrastructure, which by design, implementation or operation, has a limited assessable susceptibility to destruction or incapacitation by a threat.
- **Medium Vulnerability**. A critical infrastructure, which by design, implementation or operation, has a moderate assessable susceptibility to destruction or incapacitation by a threat.
- **High Vulnerability**. A critical infrastructure, which by design, implementation or operation, has an extreme assessable susceptibility to destruction or incapacitation by a threat.

Vulnerability assessment rankings can identify single points of failure, enable enterprises to understand their highly complex infrastructures, and help critical infrastructure sectors to address deficiencies in an expeditious and cost effective manner.

4.1.2 Threats

A threat is a set of circumstances that has the potential to cause loss or harm. A threat source may be an individual, an organization, a nation, or a natural or accidental event that possesses the capability to exploit a critical infrastructure's security [74]. There are two main categories of threats to information systems: intentional threats and inadvertent threats. Intentional threats involve acts deliberately taken to breach security. Inadvertent threats involve situations where security is threatened by natural forces or by human actions that are not intended to breach security but still adversely affect the information systems. Figure 4.1 presents the different types of intentional and inadvertent threats to information systems within each critical infrastructure [35].

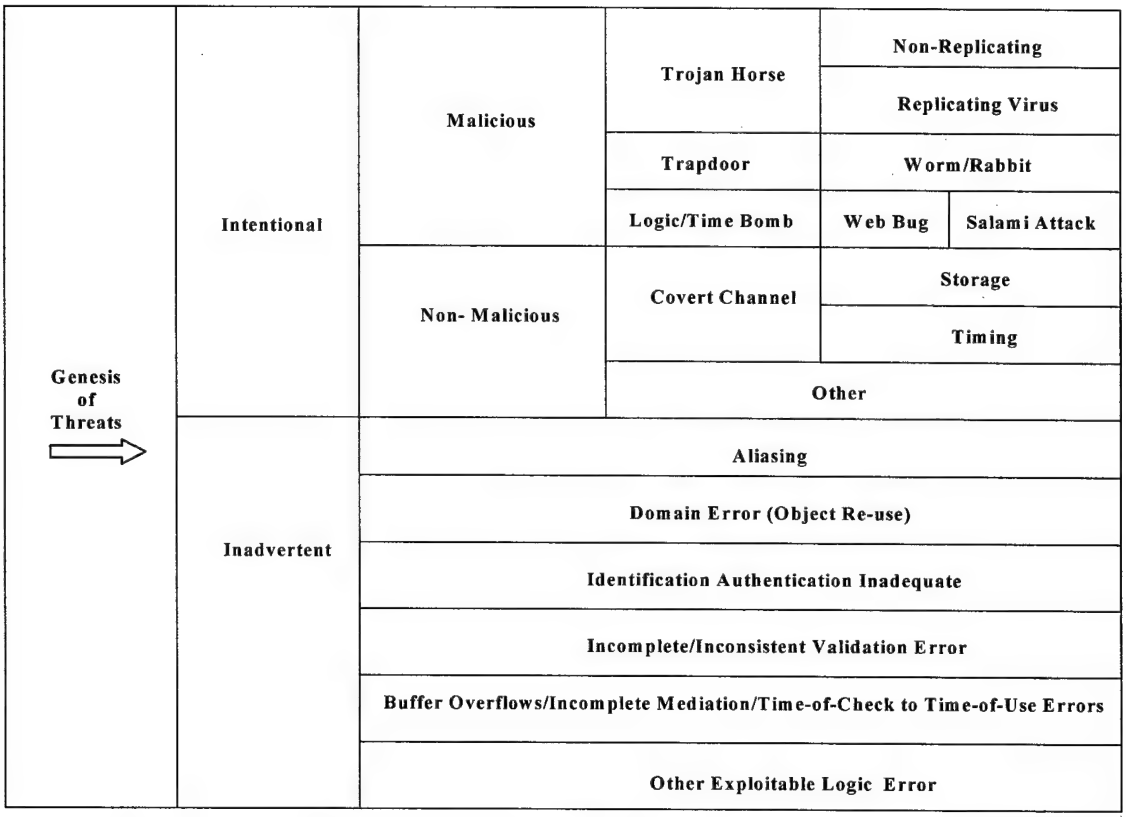

Figure 4.1: Genesis of Threats.

Threats can compromise the confidentiality of a system through unauthorized disclosure, rights usage or communications interception. Threats also affect the availability of data and services. Threats to the information and telecommunications critical infrastructure sector can degrade communications and disrupt data processing with potentially catastrophic consequences.

Enterprises must ensure that their systems are secure by researching and assigning values to all known threats. One method of analyzing threats is through a qualitative measurement matrix, similar to that for assessing vulnerabilities. The definitive characteristic of the qualitative approach is the use of ordinal rankings, which include the following threat categories [74]:

- **No Threat**. No potential for an individual, organization, nation, natural or inadvertent event, to exploit vulnerabilities with the malicious intent of causing a disruption or destruction to critical infrastructures.
- **Low Threat**. Limited potential for an individual, organization, nation, natural or inadvertent event, to exploit vulnerabilities with the malicious intent of causing a disruption or destruction to critical infrastructures.
- **Medium Threat**. Moderate potential for an individual, organization, nation, natural or inadvertent event, to exploit vulnerabilities with the malicious intent of causing a disruption or destruction to critical infrastructures.
- **High Threat**. Extreme potential for an individual, organization, nation, natural or inadvertent event, to exploit vulnerabilities with the malicious intent of causing a disruption or destruction to critical infrastructures.

Since eighty-five percent of all U.S. critical infrastructures are owned by the private sector, it is important that government not rely solely on its own assessments of threats. State and local operators of critical infrastructures cannot develop defenses without fully understanding what they are defending against. Cooperative industry and government threat assessments can allow critical infrastructure sectors to focus on defending known deficiencies in an expeditious and cost efficient manner.

4.1.3 Risk

There is no silver bullet to protect critical infrastructures; therefore, the need to manage risks to these systems is paramount. Risk is a function of probability and severity of undesirable impact—that a particular threat will exploit a particular

infrastructure's vulnerabilities. Risk can further be defined to account for seasonal, temporal and geographic variables [74]. For example, temporal factors affect how long information must be safeguarded. Similarly, risk can escalate during certain business events or during certain religious events that occur each year. It is important to consider these independent variables when calculating risk. By computing risk, while simultaneously comparing threats to vulnerabilities, the impact on each critical infrastructure sector can be determined. Figure 4.2 presents one method of how risk is computed in relation to both threats and vulnerabilities [74].

		Vulnerability Assessment			
		None	Low	Medium	High
Threat Assessment	None				
	Low				
	Medium				
	High				

$$R = f\,(P\,(T * V), I, s, t, g)$$

Legend:
R = Risk
F = Function
P = Probability
T = Threat
V = Vulnerability
I = Impact
s = Seasonal variables
t = Temporal variables
g = Geographic variables

Figure 4.2: Risk Equation.

4.1.4 Attacks

An attack on computer systems has three primary characteristics. First, it is made up of a series of steps taken by an actor or actors. Among these steps is an action directed at a target through the use of some tool to exploit a vulnerability. Moreover, an attack is intended to achieve an unauthorized result. An unauthorized result is any

adverse event whereby some aspect of the security of the system is violated [35]. Thus, an attack is the culmination of a series of intentional steps initiated by the attacker that allows increased access, disclosure of information, corruption of information, denial of service or the theft of resources. This differentiates an attack or malicious incident from an inadvertent action [35]. Figure 4.3 presents the five logical steps involved in an attack [35].

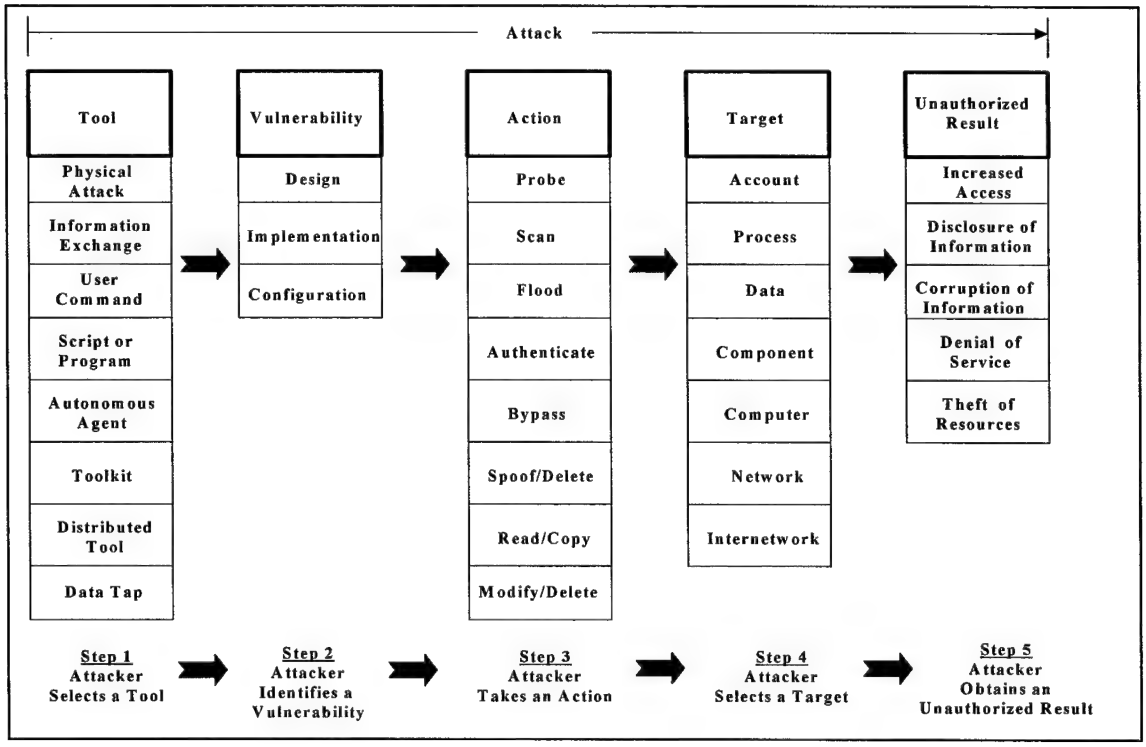

Figure 4.3: Five Steps of a Computer System Attack.

Attacks on America's critical infrastructures have not only affected computer controlled systems for the electrical and telecommunications sector, but also vital databases that contain medical records, criminal records and proprietary industry information. For example, two of America's largest states (i.e., Florida and New York) have had their 911 service disrupted, causing confusion and impacting emergency

response capabilities. Telephone service for large regions have been interrupted affecting major airports [87]. And computer viruses have moved through the Internet overloading critical infrastructure systems, shutting down major portions of corporate and government services [87]. These attacks have been very pervasive and have targeted federal, state and local governments, and the private sector. The type of attacks or misuse reported in the 2003 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) computer crime and security survey are presented in Figure 4.4 [69].

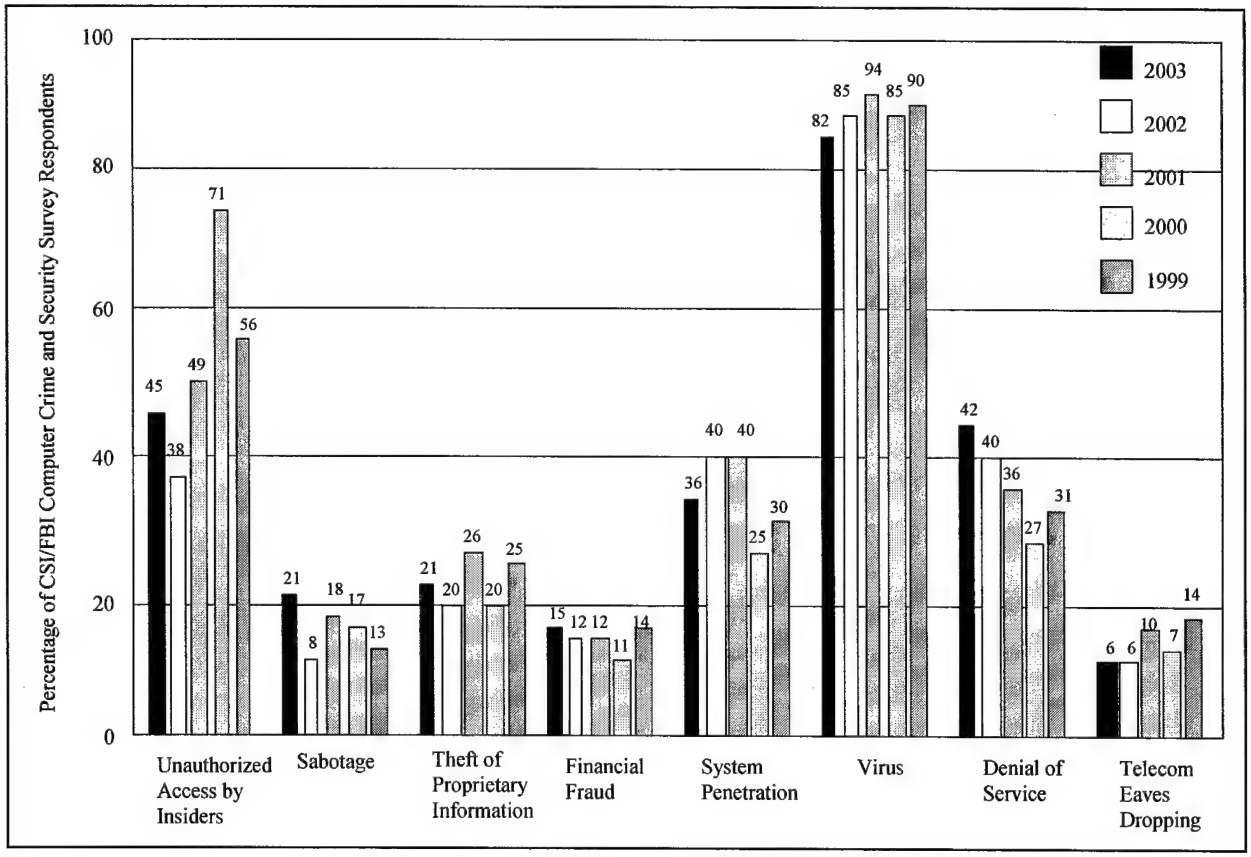

Figure 4.4: Types of Attacks or Misuse.

4.2 Cyber Attack Protagonists

Most agencies classify actors who would harm the nation's critical infrastructures into five broad groups [87]: insiders, economic competitors, hackers, transnational

entities, and nation states. According to the 2003 CSI/FBI Computer Crime and Security Survey, one of the greatest threats is from insiders [69]. The second group, economic competitors, refers to corporations and countries that attempt to obtain trade secrets, advanced technologies and research results in order to support their corporate and national agendas. The third group, hackers, refers to an unstructured, lone actor or group who is not sponsored by an outside agency such as a nation state. The fourth group, transnational entities, refers to a group that is typically structured in either cells or in autonomous groups, which have the capacity to form and swarm, then dissipate. These groups share a common agenda and are usually better funded than the lone hacker. The fifth group, nation states, are the best funded and most structured entities, with a full range of computer network attack tools and connectivity at their disposal.

4.2.1 Insiders

It is worth noting that some of the most significant damage ever done to the national security of the United States came from Aldrich Ames and Robert Hansen, both insiders. Insiders hold positions of trust and often prominence within their respective organizations. This trust allows an employee to gain access to passwords and other critical information. Disgruntled or ex-employees often possess a motive for malicious actions due to layoffs, financial disputes, or other perceived grievances. Insiders have the capability and access to disrupt interconnected information systems, to deny the use of information systems and data, and to remove, alter or destroy information. For example, of the 1,004 investigations associated with Department of Defense information systems in 2003, eighty-seven percent were either employees or otherwise internal to the organization [18]. In another instance, the 2003 CSI/FBI Computer Crime and Security

Survey reports, "insider abuse of system access as one of the most cited forms of attack" [69]. Overall, the rise of insider threats makes this disaffected group perhaps the most formidable one for the United States. The sources of insider threats can be broken down into four basic categories [18]:

- **Malice**, the intentional compromise, destruction or disruption, of information and services.
- **Disdain** for security practices that results in willful unauthorized storage, destruction, or improper handling of sensitive information, materials and computer systems.
- **Carelessness** in the use of information systems by breeching security policies and practices.
- **Ignorance** of security policies, security practices and information system use.

4.2.2 Economic Competitors

President Clinton's 1998 Annual Report to Congress on *Foreign Economic Collection and Industrial Espionage* reported that several countries are targeting America's industrial and economic information and information systems. Such espionage is being conducted not only by intelligence organizations, but also by businesses. Both groups are actively targeting U.S. citizens, industries and the U.S government to obtain information about advanced technologies [87].

Outsourcing of jobs and business processes can bring efficiencies and cut costs but they can also introduce security risks. Currently, some of the most sensitive computer

code for U.S. systems is being written overseas. The Chairman of the National Intelligence Council has warned that with as many as three million software technology jobs poised to move offshore by 2015, the United States needs to ensure that it has taken protective actions against these new potential security risks [38]. The ability of corporations to process the security clearances of individuals in these environments is also challenging.

Information technology has become as important to the United States as oil; this poses special concerns for critical infrastructure protection and the nation's security. For instance, fifty percent of the world's laptops, one quarter of the world's desktop computers and fifty percent of all personal computer motherboards are now manufactured in China [38]. Furthermore, seventy percent of all semiconductor chips (which have been designed by other countries such as the United States) are now being produced in Taiwan. Due to the migration of jobs and technology abroad, and because of the dependencies on the information and telecommunications sector, the threat of economic espionage is real and continues to grow despite the nation's adoption of the *Economic Espionage Act* of 1996.

4.2.3 Hackers

Hackers are usually unstructured, lone actors or groups who are unsponsored and typically use well-known methods and tools. Moreover, the hacker's attacks usually do not have an organizational objective. Hackers are usually capricious or eccentric in their methods, but their *modus operandi* for why they hack is fairly consistent; they hack for excitement, fame, profit, and control. The probability of attack from hackers can be very

high while the potential for damage can range from low (e.g., web page defacements) to extremely high (e.g., large scale denial of service attacks).

Hackers pursue the projection of their desires via the Internet. As hackers become politicized and as activists become computerized, state and local governments, as well as the rest of society, will see an increase in the number of cyber-activists who engage in electronic civil disobedience, also known as hacktivism [109]. For example, in 1999 the City of Seattle hosted the World Trade Organization (WTO) summit, which touched off three days of street riots by anarchists and traditional demonstrators. The "electrohippies" also participated in the WTO civil disobedience by launching coordinated electronic and street based protests. Many individuals, who could not get to Seattle, registered their dissent by slowing, blocking and disrupting access to WTO servers [7].

In another incident, a cyber battle between hacking groups erupted with the Chinese media reporting at least 600 websites attacked across the United States. In 2001, hacker groups in China conducted massive waves of attacks on websites based in the United States in protest of the collision between U.S. and Chinese military planes which left one Chinese pilot dead. Chinese activists allegedly targeted U.S. organizations, including the UPI news agency, U.S. Department of Labor, the U.S. Surface Transportation Board, the U.S. Department of Health, and other mostly non-classified government sites – all of which had direct effects on federal services to state and local governments [20].

4.2.4 Transnationals

The second category of threat is from transnationals, which is perhaps the most difficult outsider threat for federal, state and local governments to defend against. The transnational threat is constructed around a cell or an autonomous group format that allows for swarming. This group usually shares a common goal and ideology (e.g., dislike the deployment of U.S. soldiers in Saudi Arabia). The sophistication of this groups methods and tools makes them look much like the individual hacker, yet they are much more organized.

The potential damage from this group can be documented in four primary categories, which include: (i) the theft of data, (ii) the interception of data for profit (iii) the manipulation of data and (iv) the use of digital technologies to assist in the destruction of real-world assets. The first category usually manifests itself in acts of industrial espionage; the second category usually manifests itself in narco-trafficking; the third category usually manifests itself in website attacks designed to heighten ideological and political awareness of a cause; and the fourth category usually manifests itself through the use of cyber capabilities to support conventional kinetic attacks. A possible attack scenario for this group is to combine a cyber attack against a telephone switch that supports the 911 system, with a traditional kinetic attack such as a bomb. This lethal combination would not only be effective in multiplying the physical effect of the attack, but would heighten the psychological effects of the attack as well.

For example, in late 2002, Detective Chris Hsiung of the Mountain View (CA) Police Department began investigating a suspicious pattern of surveillance against

computer systems used to manage Bay Area utilities and government offices. After identifying the suspicious network traffic as coming from the Middle East and South Asia, Hsiung informed the FBI's San Francisco computer intrusion squad.

Working with experts at the Lawrence Livermore National Laboratory, the FBI found multiple casings of sites for information about emergency telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities [26].

An analysis of the probes led the FBI to conclude that a kinetic attack was being planned. In addition, some of the probes were directed against SCADA systems that allow remote control of critical services. In fact, according to law enforcement and national security officials, more information about those systems and how to program them was discovered on al Qaeda computers seized in 2002. These troubling discoveries have led some experts to conclude that al Qaeda and other groups are at the threshold of using the Internet as an instrument of terror. This new threat comes as a direct result of the convergence of computer systems and the physical structures they control. By disabling or seizing control of the floodgates in a dam, for example, a terrorist could use digital tools to destroy lives and property. Although there is limited evidence to support the idea, some analysts believe that terrorists aim to employ those techniques in conjunction with "kinetic weapons" such as traditional explosives [26].

4.2.5 Nation States

Although much publicity has been given to the transnational threat, the nation state still merits attention as it has overwhelming technical resources, financial assets and a

larger pool of intellectual capital to draw from—all of which allow for sustained efforts at a level none of the other groups can produce.

For example, the Russians have an established information warfare program. In a speech given at the Russian—U.S. Conference on Evolving Post-Cold War National Security Issues in Moscow in September of 1995, V.I. Tysmbal stated, "from a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of conflict, whether there were casualties or not" [91]. Russia has stated that it retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself, as it violates the jurisdictional integrity of Russian borders [91].

In the past decade, China's military modernization has increasingly attracted U.S. attention. In particular, the concept of information warfare has emerged in Chinese military doctrine. China's appreciation for information as an instrument of statecraft and military power has significant ramifications for the United States. Given the tremendous advances in information systems both in terms of the rate of innovation and quality of improvements, China has positioned itself to exploit this revolution in military affairs. China has surprised observers with its developments in nuclear weapons, missile and space technologies, it is similarly coming to the forefront in the information warfare arena [110].

China's focus on information warfare presents a dangerous challenge for the United States. For example, in two information warfare exercises in 1997 and 1999, the U.S. military found that state sponsored cyber-attacks using commercially available

technologies, were able to prevent the United States from staging and prosecuting military operations effectively. The Pentagon designed the first exercise around military operations on the Korean Peninsula. The result of that exercise was more than instructive; the series of attacks against civilian and military networks had a paralyzing effect on U.S. command and control affecting all levels of leadership. It is conceivable that information warfare could provide China with an asymmetric capacity to hinder U.S. military operations in the Asia-Pacific area of operations, a region of significant importance to U.S. national security interests [110].

In summary, America's networked information systems and the critical infrastructures that they support are within the capability and interests of adversaries who would do them harm. As such, America, especially at the state and local level where essential services are delivered, must evaluate the vulnerabilities, threats and risks to their critical infrastructures in order to prevent them from being disabled or disrupted. Figure 4.5 presents the 2003 CSI/FBI Computer Crime and Security Survey synopsis on sources of attack [69].

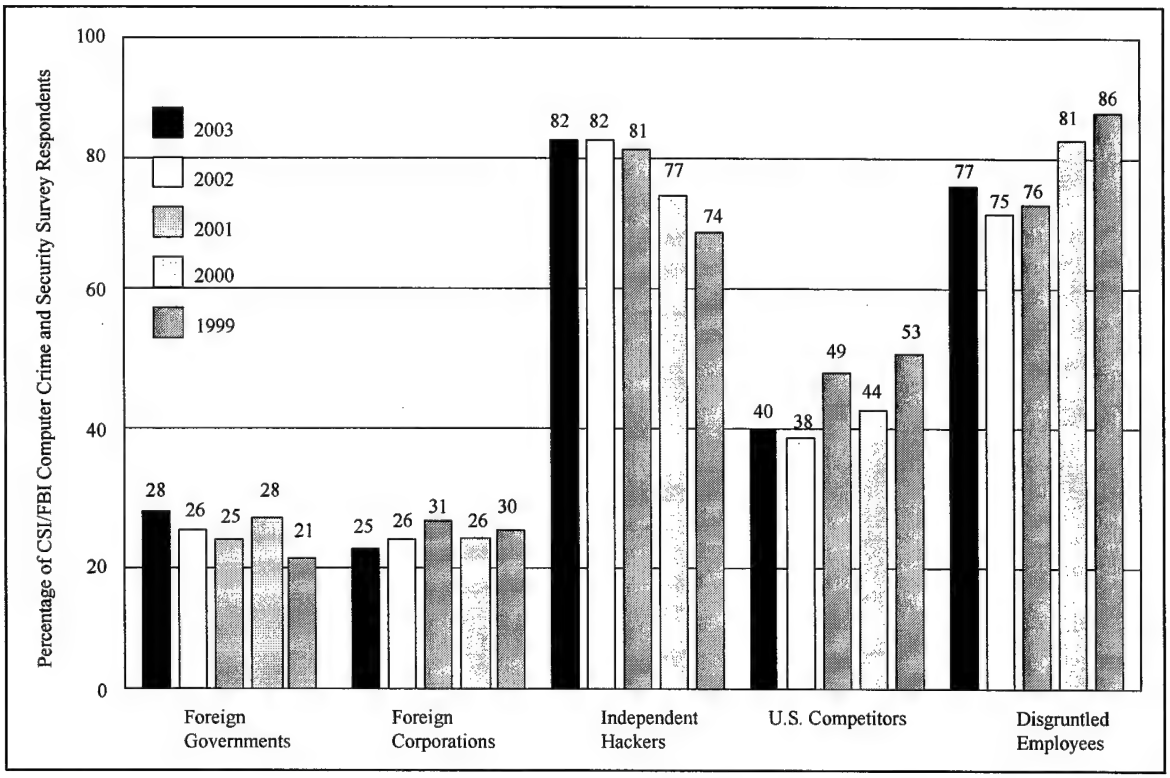

Figure 4.5: Sources of Attack.

CHAPTER V

DEFENSE IN DEPTH: TECHNOLOGY

Frederick the Great reminded military planners that it is impossible to defend against every attack. For centuries, it has been a principle of warfare that no defense can be absolutely impregnable. Layering defenses and surrendering them gradually to create time and space between friendly and hostile forces was an idea well known in the Middle Ages. Villages were strategically placed around the castle so that they presented "stumbling blocks" to the enemy. If these defenses were breached, castle walls and a moat around the castle acted as additional layers of defense [39]. Evolution of this concept, known as defense in depth, occurred between the 11th and 13th centuries and eventually included crosswalks, slotted walls and a strong gatehouse, adding even more layers to the castle defense [40].

The idea behind defense in depth is to cause an adversary who might penetrate one defense to immediately encounter another, then another, until the attack is deterred. Frank Hayes, *Computer World* columnist, affirms the defense in depth concept with his now famous quote, "the best defense is a lot of defense" [34].

A good goal for enterprises at all levels is to develop defense in depth for information technologies whereby each layer of security builds on the next—much like the walls, moat, and interior chambers that make up a castle system. Defense in depth can be realized at a global level for enterprises by weaving technology, legislation and

policy to establish a multi-layer, multi-dimensional protection system—like the defenses of a castle. The next three chapters examine these constructs beginning with an investigation of the technologies useful in countering the attacks presented in Chapter IV.

5.1 Enterprise Security Management

Effective enterprise security management underlies any successful critical infrastructure protection program. The principal goal of an organization's enterprise security management process is to manage risk by limiting vulnerabilities, protecting against threats and limiting the impact of attacks. Therefore, enterprise security management should be treated as a technical and operational function to be implemented by the experts who operate and manage the IT system, and as an essential senior-level management function that sets strategic security goals of the organization [79].

Enterprise security management supports critical infrastructure protection by securing the information systems that store, process, or transmit enterprise information. Also, it enables enterprises to make better-informed IT management decisions and assists management in certifying and accrediting enterprise information systems [79].

Enterprise security management operates primarily on three levels: (i) the operational level that defines the procedures and uses of technology, (ii) the managerial level, which sets the policies expressing how an enterprise's technologies are to be utilized, and (iii) the technology level, which further defines the security controls for the enterprise. Enterprise security controls may range from simple to complex, involving hardware, software and personnel controls. All of these measures should support each

other to effectively secure critical infrastructure components. Technical controls can be grouped into the following major categories [79]:

- **Preventive Controls** focus on preempting security incidents from occurring in the first place (e.g., access control).
- **Detect and Recover Controls** focus on identifying and reconstituting from a security incident (e.g., disaster recovery).
- **Supporting Controls** are generic measures that underlie most information security capabilities. These measures must be in place in order to implement other procedures (e.g., continuity of operations).

Enterprise security management should address the greatest risks while simultaneously striving for adequate mitigation at the lowest cost to ensure the least possible impact to the organization's mission. Figure 5.1 depicts the primary enterprise security management phases and the relationships between them [79].

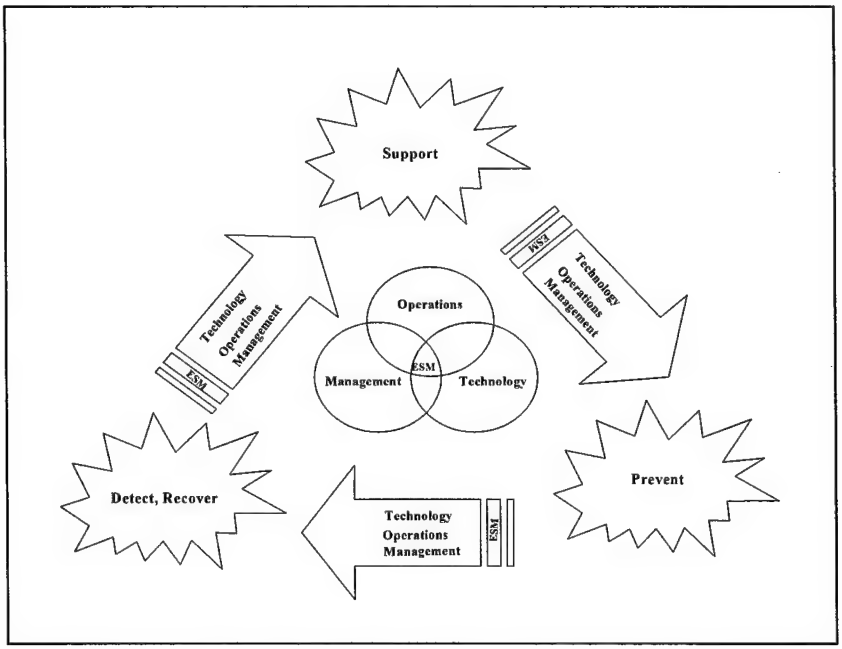

Figure 5.1: Enterprise Security Management Phases.

5.2 Technology Components

To produce an effective technological cyber defense layer, each enterprise must apply information assurance techniques to safeguard its "keep." Information assurance is defined as information operations that defend and protect both the information system and the information on that system by ensuring their availability, integrity, authentication, confidentiality and non-repudiation [68].

- **Availability** ensures that assets are accessible to authorized users at the appropriate time. Availability can also be understood by its opposite—denial of service or performance degradation.
- **Integrity** ensures that assets can be modified only by authorized users in authorized ways.
- **Authentication** ensures that users who request access to an object are indeed who they claim to be. Authentication establishes and verifies a user's identity.
- **Confidentiality** ensures that only authorized users access computer assets. Confidentiality can also be defined as secrecy.
- **Non-Repudiation** ensures that a user cannot deny having made a transaction.

Information assurance is the layered security strategy that counters a full range of attacks by defending in multiple places. It increases resistance to security threats by protecting against interception, interruption, modification, and fabrication [68].

- **Interception** occurs when some unauthorized party has gained access to an asset (e.g., wiretapping or illicit copying of data).

- **Interruption** occurs when an asset of a system becomes lost, unavailable or unusable (e.g., malicious erasure of a program file).
- **Modification** occurs when an unauthorized party not only accesses an asset but tampers with it as well (e.g., altering a program to perform additional computations).
- **Fabrication** occurs when a subject creates a fake object on a computing system (e.g., injecting or adding records to a database).

In the event that information assurance fails to produce an effective defense, an enterprise must apply digital forensic techniques to analyze the compromises to its information systems. Digital forensics is defined as the scientific collection and analysis of data from computer storage and network media for use as evidence in a court of law [17]. The essential elements of digital forensics includes [17]:

- **Collection**, the secure retrieval of computer data.
- **Examination**, the stateful inspection of suspect computer data to determine details such as origin and content.
- **Presentation**, the legal and proper introduction of computer based information in legal proceedings.
- **Application**, the adaptation and evolution of prevailing laws to computer practices and technology.

Like the medieval castle system, today's defenders must use every available means to protect against the threats to critical infrastructures. Technical security measures

include cryptography, passwords, tokens, biometrics, digital signatures, firewalls, intrusion detection systems, malicious code/virus detection and removal programs, proxy servers, system monitoring tools, redundant multiple data paths and backup systems. The aforementioned security controls can be grouped into the following areas: (i) hardware controls, (ii) software controls, (iii) physical protection controls, and (iv) human controls.

5.2.1 Hardware Controls

The vital systems that operate and link America's critical infrastructures must be protected. One component of those systems is computer hardware. Hardware includes elements such as (i) processors, (ii) memory, (iii) input/output devices and (iv) also network devices. Some of the important hardware technologies used to protect critical infrastructure networks include [40]:

- **Automated Tools for Monitoring and Management** have the capability to detect intrusions, disruptions and degradations that indicate potential security problems. An important class of automated monitoring tools are intrusion detection systems (IDSs). An intrusion detection system inspects inbound and outbound network traffic and identifies suspicious patterns that may indicate a network or system attack. In addition to detecting attacks, IDSs also provide forensic information about attacks. IDSs are primarily signature-based (i.e., scanning for specific known attacks) or anomaly based, (i.e., detecting deviations from a baseline or normal state of the network).

- **Firewalls** screen out traffic based on criteria such as sender or destination address, and may be implemented in hardware or software. A firewall does not

normally signal an attack from inside a network. In contrast, an IDS system evaluates traffic from both inside and outside a network, signaling an alarm once a suspected intrusion has taken place.

- An **Application Proxy** blocks or filters user requests at the application level. Application proxies enforce security policies by limiting user access from unauthorized sites.

- **Cryptography** is the science of protecting information by encrypting or transforming it into an unreadable format, called cipher text. Only those users who possess a secret key can decipher the message back into its original form, called plaintext. Cryptographic systems can be either hardware or software. Cryptographic systems are broadly grouped into two types, symmetric key systems (i.e., that use a single key that the sender and recipient share) and public key systems (i.e., that use two keys, a public key known to everyone and a private key only known to one individual) [68]. Modern cryptographic algorithms are virtually unbreakable by brute force attacks.

- **Redundant and Multiple Circuit Paths** offer more than one physical route for data transport. They ensure continued transmission when network components are degraded or disrupted. In addition to the redundant circuits themselves, contract provisions should be in place with multiple vendors to protect against denial of service attacks. Furthermore, circuit services should be procured from more than one vendor to avoid single points of failure. With today's business climate of mergers, leases and sub-leases, it is important to guarantee that

business contracts actually refer to distinct physical routes to avoid contracting for back-up capabilities on the same circuit paths.

5.2.2 Software Controls

The vital systems that link and operate America's critical infrastructures cannot be protected by hardware alone. Some of the important software technologies that help defend critical infrastructure networks are listed below [68]:

- **Strong Access Controls** include passwords, tokens and biometrics, which can support electronic access control. Electronic or logical access controls help ensure that unauthorized users do not gain access to privileged data or services. Similarly, special software tools that function within operating systems can also implement user access and privilege controls on objects such as databases.
- **Guards** are sophisticated firewalls. The degree of control that a guard can provide is only limited by what it is programmed to do. For example, a guard might be employed to support users working on a shared network with limited bandwidth to the World Wide Web. By programming the guard to disallow complex graphics and text, connection speeds for all network users can be enhanced.
- **Personal Firewalls** are application programs that run on user workstations to filter and block unwanted traffic. Personal firewalls can augment conventional network firewalls. Personal firewalls can also compensate for networks that lack regular firewalls.

- **Digital Signatures** are digital codes attached to electronically transmitted messages that uniquely identify senders. Electronic signatures are similar to written signatures and must be unforgeable. Digital signatures are an essential element of electronic commerce.
- **Malicious Code and Virus Detectors** play an important role in maintaining system integrity by identifying and eliminating harmful software. Most anti-virus programs automatically download updates to scan for new viruses.
- **Virtual Private Networks (VPNs)** allow the secure sharing of network resources across insecure channels (e.g., the Internet). VPN solutions achieve confidentiality through the use of encryption.
- **Software Certification and Accreditation** help assess the security posture of a system and how that system can affect the security posture of other systems in its environment. Software certification and accreditation provide guidance for each phase of the software engineering life cycle.

Any IT product added to critical infrastructure networks should be accredited and validated in accordance with the National Institute of Standards and Technology (NIST) or its associated certified commercial laboratories. For a system to be accredited, NIST recommends that enterprises meet the following requirements [102]:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement.

- National Security Agency (NSA)/National Institute of Standards and Technology (NIST) and National Information Assurance Partnership (NIAP) Evaluation and Validation Program.
- NIST Federal Information Processing Standard (FIPS) Validation Program.

The DoD Information Technology Certification and Accreditation process (DITSCAP) is recommended for grading the security of information systems throughout their lifecycles [22]. DITSCAP involves seven certification tasks, (i) system architecture analysis, (ii) software design analysis, (iii) network connection rule compliance analysis, (iv) integrity analysis of integrated products, (v) life cycle management analysis, (vi) security validation requirements procedures preparation, and (vii) vulnerability assessment analysis [22].

5.2.3 Physical Security Controls

One of the easiest, most effective and least expensive ways to protect critical infrastructure information systems is through the use of physical controls. Physical safeguards are security measures that protect an organization's equipment and facilities from natural environmental hazards and unauthorized intrusion. In order to guard the integrity, confidentiality and availability of information systems, the following physical security measures should be implemented [101]:

- **Facility Access Controls** limit physical access to electronic information systems and the facilities in which they are housed in order to prevent unauthorized physical access, tampering, or theft.

- **Access Control and Validation Procedures** control and validate individuals' access to facilities based on their roles or functions.
- **Maintenance Records** document repairs and modifications to the physical components of a facility (e.g., computer hardware, walls, doors, and locks) in order to prevent unauthorized modifications or tampering.
- **Workstation Security** includes measures to physically safeguard all workstations. This requirement is met by restricting access to authorized procedures and users through hardware (e.g., locks, cases or cabling) or software controls (e.g., passwords, biometrics or smart cards).
- **Media and Storage Controls** formally document the instructions and procedures that govern the receipt, installation and removal of hardware and software into and out of a facility. Physical security for storage media should also include data backups and specific disposal procedures.

Physical security measures are often the most cost effective and expedient. However, physical controls are often bypassed in favor of more sophisticated technological measures, which do not always satisfy the security needs of the organization and often conflict with the need for "remote access."

5.2.4 Human Controls

Most computer-based security incidents are caused by human factors. As such, any measures taken to protect critical infrastructure systems would not be complete without addressing this issue. Several human workforce security controls are listed below [101]:

- **Sanction Controls** involve applying the appropriate sanctions against members of the workforce who fail to comply with the security policies and procedures of the organization.
- **Implementation Controls** include authorization and/or supervision procedures for workforce members who work with electronically protected information.
- **Password Management** ensures that there are procedures for creating, changing, and safeguarding passwords.
- **Security Incident Procedures** ensures a systematic methodology for reporting and handling security incidents.
- **Minimal Privilege Controls** ensure that users only have access to information needed to perform their tasks.
- **Minimal Exposure Controls** ensure that once users have gained access to sensitive information, need-to-know procedures are applied to protect that information while it is being processed, stored or transmitted.

When security incidents occur, enterprises must respond quickly and effectively. The faster an enterprise recognizes, analyzes, and responds to an incident, the better it can limit damage and recovery costs. Establishing a computer emergency response team (CERT) is one way to provide this rapid response capability [41].

The banking and finance sector was one of the first sectors to understand the increasing interdependencies among computer systems. For example, in 1999, Deutsche Bank, which employs over 93,000 people in 60 countries, decided to formalize its responses to security incidents by creating a computer emergency response team (CERT)

to handle network attacks and incidents [41]. Deutsche Bank found that having the right personnel assigned to the enterprise's computer emergency response teams was crucial. At a minimum, the management authority team should include board level management, a chief information officer, chief technology officer and the chief information security officer. Computer emergency response teams also ensure that all actions taken are done in accordance with the business continuity plan. Computer emergency response teams have, among their myriad duties, three primary focus areas [41]:

- **Validation** is the re-examination of assigned alert levels based on the analysis of potential impacts if an alert is not broadcast and implemented.
- **Control Verification** is the assessment of current security measures and how they would respond to the threats and vulnerabilities identified by an alert.
- **Countermeasure Formulation** is the development or preparation of processes, tools and procedures to counter threats and vulnerabilities.

In summary, the ability of specific technologies to support the protection of critical infrastructures varies whether they are used alone or in combination. Moreover, the characteristics of the system and security environment they operate in are important factors that influence how critical infrastructures are safeguarded. Figure 5.2 illustrates the relationship between enterprise technical security measures and their critical infrastructure protection goals of availability, confidentiality, integrity, authentication and non-repudiation [40]:

Technical Security Measures	Availability	Confidentiality	Integrity	Authentication	Non-Repudiation
Intrusion Detection		●	●	●	●
Firewalls				●	
Proxy Server		●			
Cryptography		●	●	●	●
Passwords, Tokens and Biometrics				●	●
Guards		●	●		
Personal Firewalls				●	●
Digital Signatures				●	●
Malicious Code/Anti-virus	●	●	●		
Redundant Paths	●		●		

Figure 5.2: Technology Summary.

5.3 Project Matrix

Security measures can only be effective if, as in the castle metaphor, they are positioned properly. In order to distribute technological assets, enterprises must conduct a thorough examination of their critical infrastructures. These actions should be modeled after a federal-level program called Project Matrix [95]. Project Matrix is an effort designed to assist federal civilian agencies in prioritizing their critical infrastructure protection efforts by identifying a comprehensive list of each organization's assets, determining the relative significance of those assets, and examining how those assets affect the economic stability, critical health and public safety of government. By identifying the associated interdependencies between assets, agencies can begin to take

steps to protect their critical infrastructures. These steps could form the basis for new legislation, policies and technology controls such as recovery, back-up and fail-safe methods.

At the federal level, Project Matrix solicited the voluntary participation of 17 civilian federal departments and agencies. At the state and local levels, a Project Matrix team should comprise government agencies as well as private sector representatives from all critical infrastructure areas.

The implementation of Project Matrix involves:

- **Step 1** identifies the most critical assets.
- **Step 2** captures the major nodes and networks upon which the most critical assets depend.
- **Step 3** ties the most critical assets and their supporting nodes and networks to their underlying infrastructures.

5.3.1 Benefits of State Implemented Project Matrix

Public and private sector entities often are under the assumption that an "infrastructure will always be there." This ethos should be reevaluated. A Project Matrix performed at the state and local levels can accomplish this.

Project Matrix enables state and local entities to integrate their security needs and posture with the federal government and the private sector. Specific benefits are:

- **Asset Identification**: There will never be enough resources to secure all critical infrastructure assets from compromise. However, by providing an integrated

approach through the application of a Project Matrix, the most vital state and local assets can be identified and protected.

- **Fiscal Planning**: Balancing the fiscal realities of operating and maintaining critical infrastructure protection systems with other state needs is always a challenge. Project Matrix can help prioritize budget outlays in order to support critical infrastructure protection efforts.

- **Functional Balance**: Critical infrastructure protection systems must meet state and local goals and align with the needs of the private sector and the federal government. These are difficult tasks as a balance between security and wide-open functionality must be struck in order to support the myriad of state and local user requirements.

- **Legislative Support**: The ebb and flow of political leadership within state and local governments present challenges for critical infrastructure protection. Budgeting support for state and local computer security measures can vary considerably. A Project Matrix can help maintain critical infrastructure security as a leadership priority within state and local level governments.

- **Survivability and Profitability**: Balancing network redundancy and reliability to support critical infrastructures with private enterprises' need to maintain profits and stock values can be challenging. A state and local level Project Matrix can highlight the need for critical infrastructure protection in industry through security awareness campaigns aimed at the local populace.

- **Training and Staffing**: Sufficient numbers of trained personnel must be available to protect state and local level critical infrastructures. A Project Matrix can help secure the necessary legislative support in order to create and maintain a well-trained workforce.

- **Partnerships**: Eighty-five percent of all critical infrastructures are owned by the private sector. It is essential, therefore, that partnerships be developed between the private sector and state and local governments.

In summary, the benefits of a state and local level Project Matrix approach include permitting state and local governments to define their critical infrastructure protection challenges, thereby allowing for the implementation of cost effective solutions in a structured, timely manner. In addition to cost efficiency, a state and local level based Project Matrix would permit state and local governments to identify and their most significant critical infrastructure vulnerabilities, providing the necessary framework for informed critical infrastructure protection decisions. Finally, a Project Matrix at the state and local level would provide specific information needed for constructive public/private sector discussions to address key issues of public health, safety, law enforcement, transportation and public confidence.

CHAPTER VI

DEFENSE IN DEPTH: LEGISLATION

Like the dynamically evolving defenses of medieval castle systems, legislatures must continue to take steps toward creating computer crime and anti-terrorism laws needed to mitigate and prosecute cyber incidents. If an attack is perpetrated, the law must allow for strong legal tools to prosecute and bring to justice those responsible.

6.1 Significant Legislation and Federal Guidelines

State and local legislators frequently look to federal legislation and guidelines when crafting legislation. The primary federal statute for computer crime was enacted specifically by Congress to protect computers and the information they contain. This law, the *Computer Fraud and Abuse Act* (United States Code, Title 18, Section 1030) contains six separate offenses, three of which are felonies and three of which are misdemeanors [10].

The first felony protects classified information and is contained in Title 18, Section 1030(a)(1). This section was designed to prohibit the unauthorized access of classified information on a system. The second felony is contained in Title 18, Section 1030(a)(4). This section seeks to punish those who use computers in schemes to defraud others. The third felony also protects federal-interest computers. Under Title 18, Section 1030 (a)

(5)(A)(i-iii), it is a felony to knowingly cause the transmission of a program, information, code or command that intentionally causes damage [10].

The statute also provides three misdemeanors. The most significant misdemeanor protects government computers and is a strict trespass provision. The second misdemeanor protects financial information (e.g., bank records, credit card information and credit reporting services information). The third prohibits trafficking in passwords or similar information through which a computer may be accessed without authorization.

Other key legislation includes wire fraud and copyright laws, and the *Electronic Communications Privacy Act of 1986*. The *Electronic Communications Privacy Act of 1986*, Sec. 2511, has several provisions pertinent to computer crimes. For example, Section 2511(1)(a) prohibits the intentional interception and disclosure of wire, oral or electronic communications. Any violation of this statute is a felony.

The recently enacted *USA PATRIOT Act* also deals with computer security and cyberterrorism, giving investigators new authority and strengthening the penalties for cyber crime. The following bullets summarize a number of relevant sections [19].

- **Section 210: Scope of Subpoenas for Records of Electronic Communications.** Broadens the types of records that law enforcement can subpoena from Internet Service Providers (ISPs). Law enforcement can now obtain ISP information such as means and sources of payment, telephone records of sessions and temporarily assigned IP addresses.

- **Section 212: Emergency Disclosure of Electronic Communications.** Permits ISPs to disclose voluntarily stored electronic communications of subscribers (e.g., stored e-mail and other customer information) in the event imminent danger, death or serious personal injury requires such disclosure.

- **Section 213: Authority for Delaying Notice of Execution of a Warrant.** Broadens the authority of law enforcement to delay notification of search warrants in criminal investigations if prior notification would have an adverse effect and if notification is given within a reasonable period after search.

- **Section 216: Authorities Relating to the Use of Pen Register and Trap and Trace Devices.** Further modified the existing *Electronic Communication Privacy Act*. It clarified that: (i) pen/trap registers and trace authority now apply to Internet traffic, and (ii) federal courts' issuance of *ex parte* orders authorizing the use of pen/trap registers are now valid anywhere within the U.S., essentially creating national subpoenas.

In addition, the *USA PATRIOT Act* now treats stored voice mail like stored e-mail (rather than telephone conversations), eases government access to confidential information, and authorizes "sneak and peek" (e.g., no notice) search warrants.

In summary, the *USA PATRIOT Act* greatly expands the powers of law enforcement. It allows greater freedom and scope of efforts such as searching through e-mail and Internet traffic, placing wiretaps and conducting other forms of electronic surveillance.

6.2 State Computer Crime Laws

In addition to the applicable federal statutes, state law must also be considered. States revisit their computer crime laws and change them much more frequently than their federal counterparts. The diversity and variety of enactments are discussed by Anne W. Branscomb in *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime,* published in the Rutgers Computer and Technology Law Journal [4]. Her study was dedicated predominantly to assessing how adequately existing laws address problems presented by rogue programs or intrusive code. Branscomb distilled from existing enactments ten specific ways in which states have acted to create computer crime legislation. Important features of Branscomb's taxonomy, which has been adopted by a number of authoritative sources, are [4]:

- **Expanded Definition of Property**. Branscomb noted that a few states reacted to the threat of computer crime by including, within their respective definitions of property, information in the form of electronic impulses or data, whether tangible or intangible, either in transit or stored.

- **Unlawful Destruction**. Many states have criminalized activities that alter, damage, delete, or destroy computer programs or files. Branscomb noted that such prohibitions, standing alone, might not always reach the problem of intrusive code, which may be introduced without immediate alteration of existing files and programs.

- **Use of a Computer to Commit, Aid, or Abet the Commission of a Crime**. Laws of this type were passed to prohibit the use of a computer to facilitate other crimes, such as theft or fraud.

- **Crimes Against Intellectual Property**. Laws in this category include offenses from the perspective of the information being protected. For example, some laws were passed to define offenses involving the destruction, alteration, disclosure, or use of intellectual property without consent.

- **Knowing and Unauthorized Use**. Other statutes sought to criminalize acts of knowing and unauthorized use of computers or computer services.

- **Unauthorized Copying**. Statutes in this category were enacted to criminalize the unauthorized copying of computer files or software and the receipt of goods so reproduced.

- **Prevention of Authorized Use**. Branscomb noted that approximately one-fourth of states criminalized interference with, or prevention of computer use by, authorized parties.

- **Unlawful Insertion**. These laws, common to a handful of states, prohibit the unauthorized insertion of data without regard to damage resulting there from.

- **Voyeurism**. These statutes cover what is most akin to an electronic trespass. That is, they traditionally deal with unauthorized entry, without regard to damage or the resulting harm. Notably, however, some states expressly exclude mere trespass from criminal sanction.

- **Taking Possession**. Certain statutes have criminalized the taking possession of a computer or computer software.

It should be apparent that state enactments can be broader and more flexible than corresponding federal laws. They are without doubt more frequently amended, thus permitting rapid response to specific problems arising from changing technologies [4].

In summary, nearly every state has statutes banning unauthorized access and intrusions, and at least sixteen states ban unleashing harmful computer viruses and contaminants. According to the 2003 National Conference of State Legislatures, at least eight states have pending legislation that addresses cyberterrorism. In 2002, fourteen states had pending legislation that addressed cyberterrorism. At least three states—California, Georgia and Pennsylvania—have laws specifically aimed at electronic terrorist threats or acts. These statutes are summarized below [54]:

- **California Penal Code Section 11418.5**. Any person who knowingly threatens to use a weapon of mass destruction, with the specific intent that the statement, made verbally, in writing, *or by means of an electronic communication device*, is to be taken as a threat.

- **Georgia Penal Code Section 16-11-37.1**. It shall be unlawful for any person knowingly to *furnish or disseminate through a computer or computer network* any picture, photograph, or drawing, or similar visual representation or verbal description of any information designed to encourage, solicit, or otherwise promote terroristic acts.

- **Pennsylvania Penal Code 18 Pa.C.S. Section 2706**. A person commits the crime of terroristic threats if the person communicates, either directly or indirectly, a threat to: commit any crime of violence with intent to terrorize another; cause evacuation of a building, place of assembly or facility of public transportation; or otherwise cause serious public inconvenience, or cause terror. The term *"communicates" means, conveys in person or by written or electronic means, including telephone, electronic mail, Internet, facsimile, telex and similar transmissions.*

As exemplified by the above state statutes, there are many different state cyber laws across the nation. Unlike other criminal acts, computer crime and terrorism do not always occur within a single jurisdiction. It is essential, therefore, that states work together to organize new legal boundaries in the virtual domain.

6.3 Creating Uniform Legislative Acts

A logical place for states to turn for help in creating uniform acts is the National Conference of Commissioners on Uniform State Laws (NCCUSL), now in its 113th year. This influential body is comprised of more than 300 law professors, lawyers, judges and legislators appointed by the states as well as the U.S. Virgin Islands, Puerto Rico and the District of Columbia. NCCUSL has been used in the past to develop uniform laws, promote the merits of uniformity among the states and explore the best way to effect uniformity of laws between increasingly inter-dependent states. As recently as 2002, amendments to the *Uniform Computer Information Transactions Act (UCITA)* were approved by the NCCUSL at its 111th Annual Meeting held in

Tucson, Arizona. The process of drafting uniform acts is lengthy and deliberate, yet it is immensely cost-effective for states. Since its inception, NCCUSL has drafted more than 250 uniform laws on numerous subjects, including cyberspace security [51].

Comprehensive and uniform laws are needed to protect the nation's critical infrastructures. These laws must be consistently reviewed and revised, and new legislation must be crafted to keep up with advancing technology and new attacks on critical infrastructure components launched by those who would harm the nation.

CHAPTER VII

DEFENSE IN DEPTH: POLICY

The creation and implementation of sound policy is essential for critical infrastructure protection. Security policy formally articulates requirements in terms of what must be protected, how resources are to be used and what must be done. Simply stated, effective policies facilitate critical infrastructure protection through the establishment of goals, actions, procedures and standards.

7.1 Federal Policy

The federal government alone cannot protect the nation's critical infrastructure. Private industry and state and local government entities own or control the vast majority of infrastructures vital to the nation's security and economic well-being. This is not to say that the federal government does not play a significant role in infrastructure protection. It is the federal government's role to set policies to share information about potential threats, spur research and development efforts to address vulnerabilities, provide incentives to the private sector and enact regulatory constraints to ensure that assets are protected. Indeed, the federal government must provide national leadership in critical infrastructure protection.

7.1.1 Presidential Decision Directive 63

In May 1998, President Clinton issued *Presidential Decision Directive 63 (PDD 63)* to protect the physical and cyber components of America's critical infrastructures. *PDD 63* was a broad, sweeping directive that identified areas critical to the security and well being of the country and enlisted the private and public sectors in the protection effort. As outlined in Chapter III, the main areas (sectors) identified by *PDD 63* included transportation, power, water, banking and finance, information and communications, emergency management services, national defense, intelligence and foreign affairs.

Critical infrastructure services across the country are increasingly dependent on information technology. These dependencies cause the infrastructure to be highly susceptible to cyber attacks. *PDD 63* envisioned a national early warning system coupled with an emergency response capability. This national cyber warning center would rely on law enforcement, the private sector and the Department of Defense to issue warnings, detect and protect against attacks and coordinate defense actions. *PDD 63* was an excellent policy effort and is considered to be the foundation of all of America's critical infrastructure protection strategies.

However, as visionary as *PDD 63* was, the deadline of five years it set for protecting the nation's critical infrastructures was not achieved. The difficulty in achieving the five-year goal was partly due to the start-up process of developing sector plans. Each critical infrastructure sector was assigned a lead agency to work with their private sector counterparts to develop a critical infrastructure protection plan; the resulting sector plans varied in completeness and complexity. Although *PDD 63* was

inventive in its design, it failed to provide clear objectives, timetables and metrics for infrastructure security [47]. Nevertheless, *PDD 63* is one of the best critical infrastructure policy efforts ever produced.

7.1.2 Executive Order 13231

In October 2001, President Bush issued *Executive Order 13231 (EO 13231)*, which authorized a program for securing America's information systems and underlying infrastructures. *EO 13231* continued and extended the infrastructure protection efforts of its predecessor, *PDD 63*. Indeed, *EO 13231* helped the nation maintain its doctrinal foundation for critical infrastructure protection.

However, several policy recommendations of *EO 13231* have not been implemented as yet [94]. *EO 13231* called for the identification of national assets, but to date, no process for accomplishing this task has been finalized, let alone implemented. In addition, corrective actions to address security issues identified by previous critical infrastructure audits have not been undertaken. Moreover, quantifiable critical infrastructure performance measures have yet to be developed. Nevertheless, the Bush administration should be commended for *EO 13231*, which maintains and enhances the visionary strategies of *PDD 63*.

7.1.3 National Strategy for Homeland Security

The *National Strategy for Homeland Security* released in July 2002 outlined the need to prevent terrorist attacks, reduce vulnerabilities, and perform consequence

management actions necessary to minimize and recover from attacks. In particular, the *National Strategy for Homeland Security* outlined eight major initiatives [88]:

- Unify infrastructure protection efforts in the Department of Homeland Security.
- Build and maintain an accurate assessment of key critical infrastructure assets.
- Enable partnerships with state and local governments and the private sector.
- Develop a national infrastructure protection plan.
- Secure cyberspace assets.
- Harness modeling tools to develop effective protective solutions.
- Guard critical infrastructure and key assets against insider threats.
- Partner with the international community to protect infrastructures.

Policy documents ranging from *PDD 63* to the *National Strategy for Homeland Security* have recommended the compilation of national critical infrastructure components across all sectors. However, comprehensive "cross-sector" asset inventories have been difficult to conduct [47]. Also, the *National Strategy for Homeland Security* assumes that free market forces are sufficient to safeguard the nation's critical infrastructures. However, a Brookings Institution report [59] observes that most industries will not invest in infrastructure protection because they are more concerned about profits than the possibility of terrorist attacks. In fact 92 percent of surveyed executives from the nation's largest companies do not view their enterprises as potential terrorist targets [47]. Nevertheless, the *National Strategy for Homeland Security* is significant in that it focuses attention on the task of infrastructure protection.

7.1.4 National Strategy to Secure Cyber Space

The *National Strategy to Secure Cyberspace,* released in February 2003, stands out as the only policy document that focuses entirely on securing the electronic assets that underlie critical infrastructures. In particular, the *National Strategy to Secure Cyberspace* identifies five national priorities [86]:

- Creation of a national cyberspace security response system.
- Creation of a national cyberspace security threat and vulnerability reduction program.
- Creation of a national cyberspace security awareness and training program.
- Creation of a national security and international cyberspace security cooperation program.
- Creation of a national program to secure government's cyberspace.

A major recommendation is the establishment of a central authority to oversee the nation's homeland security efforts, that until recently were spread between twenty-two different federal agencies at the federal level. The Department of Homeland Security (DHS) was created to consolidate federal efforts, leadership and provide guidance to state and local entities. The National Cyber Security Division (NCSD) in DHS's Information Analysis and Infrastructure Protection (IAIP) Directorate is charged with coordinating the implementation of the *National Strategy to Secure Cyberspace*. NCSD serves as the focal point for all public and private sector efforts in the cyber security realm [96].

However, the *National Strategy* offers few incentives or regulatory requirements to motivate private sector compliance. Also, it lacks clear funding sources and budgetary plans. For example, the senior vice president and chief security counsel at Solutionary Inc., expressed concern on spending money on security initiatives without a specific action plan [23]. Moreover, the *National Strategy* focuses mainly on security recommendations for federal agencies; recommendations for corporations, universities and other organizations are much less developed [64].

It is important to note that early drafts of the *National Strategy to Secure Cyberspace* had more stringent recommendations than the final version, which has been criticized as being relatively watered down. The final version of the policy document was produced as a consensus because the recommendations in earlier versions were deemed to be too costly to be implemented by the private sector [64].

7.1.5 National Strategy for the Physical Protection of Critical Infrastructures

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* published in February 2003 outlined the need to secure the nation's critical infrastructures and assets deemed vital to public health and safety, national security, governance, economy and public confidence. It articulates eight national priorities [85]:

- Assure public safety, public confidence and services.
- Establish responsibility and accountability.
- Encourage and facilitate partnering among all levels of government and between government and industry.

- Encourage market solutions and compensate for market failure with focused government intervention.
- Facilitate information sharing.
- Foster international cooperation.
- Develop technologies and expertise to combat terrorist threats.
- Safeguard privacy and constitutional freedoms.

Unfortunately, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* discusses the implementation of critical infrastructure protection in broad terms [47]. Specific actions and timetables for critical infrastructure protection tasks are conspicuously absent. Moreover, while the policy document recommends incentives to stimulate private sector efforts, it does not provide details about the incentives and their implementation plan.

7.1.6 Analysis of Federal Policy

Even a cursory analysis of the five national policy documents reveals a major deficiency—they essentially ignore the importance of state and local entities in critical infrastructure protection. In fact, only two of the fifty-eight pages in the *National Strategy to Secure Cyberspace* deal with critical infrastructure protection issues of relevance to state and local entities.

Americans have always looked to the federal government to protect them from foreign threats. But the terrorists who attacked America on September 11, 2001 did not strike from outside the United States: they met in San Diego parks, trained in Florida and

Arizonian flight schools and launched their attacks from America's airports [73]. They were embedded in American communities. It is understood and appreciated that federal officials are coordinating twenty-two agencies in what is now the Department of Homeland Security, are trying to reform the FBI and are attempting to integrate the 100 agencies and 88 Congressional committees and subcommittees involved in critical infrastructure protection and homeland security into a homogeneous and functional group [73]. Still, it is crucial that federal policy efforts—in homeland security as well as cyber security—involve and empower state and local agencies.

To address this issue, state and local leaders need to change the way the federal government views state and local agencies. State and local governments must insist that major policy efforts are written in a "joint policy" environment. Joint policy making and coordination ensures that the knowledge and strengths of state and local entities are available to federal workers who may not have experience with state and local issues. For example, first responders are more than just the police, fire departments and health officials that arrive at the scene of a local disaster. They are literally "first defenders" against the war on terrorism [73]. Joint policy efforts can help ensure participation and buy in, leading to stronger policy and a safer nation.

Most states and cities are not significantly better prepared to react to a disaster than they were prior to September 11. If disgruntled employees or disaffected persons can potentially disrupt air traffic control systems or disable 911 emergency systems, it is not difficult to imagine terrorists doing the same [61].

The federal government should fund state and local entities to fulfill its Constitutional responsibility "to provide for the common defense" [61]. Federal funding for state and local entities could support a variety of initiatives such as [61,71]: nontraditional denial and deception measures to thwart computer based terrorist activities; Funding to hire personnel with the right technical expertise to complete critical infrastructure vulnerability assessments; The establishment of a local intelligence "network" through which federal, state and local law enforcement in every jurisdiction could share information instantly and routinely; "Networked" state and local hospitals, providing real time geo-mapped information on symptoms encountered in emergency rooms and by ambulatory services on the street. Finally, federally funded DHS positions for all fifty states at DHS headquarters would go a long way in increasing state coordination and policy making. Federal policies should reflect that state and local governments are not only the first line of defense, they are often the last. The nation's communities depend on integrated policies to protect them at home.

7.2 Role of State and Local Government Policy

State and local security policies are intended to protect the integrity of critical systems and mitigate the risks and losses associated with security threats to critical infrastructure networks and network resources.

The loss, corruption of data or unauthorized disclosure of information on state and local systems could greatly hinder vital operations. State and local governments also have a legal responsibility to secure their systems and networks from misuse. Failure to exercise due diligence may lead to financial liability for damage done by persons

accessing the network from within or without the state. The goals of state and local government security policies should include the establishment of [12]:

- Security policies that are documented, deployed and visibly enforced.
- Mechanisms to protect state and local governments; by satisfying legal and ethical responsibilities with regard to its systems.
- Policies that define rules and regulate how to protect information and computing systems.
- Statewide policies to protect critical systems from damage related to poor security practices.
- Policies to enhance information security awareness, including ensuring that users understand the consequences of noncompliance.
- Mechanisms that aid in the identification and prevention of security related abuse of critical networks and systems.
- Policies directing security and control issues.
- Policies on installation and use of hardware and software.
- Mechanisms for responding to external complaints and queries about real or perceived security related abuses of critical networks and systems.

7.3 State/Local Chief Information Officer

One of the most effective ways to implement policy is through the establishment of a single information technology and security focal point. This single individual or office should have the responsibility for the development, maintenance and enforcement of all

security policies and procedures. For state and local governments, this focal point should be the Chief Information Officer.

A Chief Information Officer (CIO) is the lead agent for all information technology and critical infrastructure policies for an enterprise. A State CIO should be a cabinet-level position that reports directly to the Governor on all IT issues. Typically, a State CIO is responsible for managing and directing all technology efforts within the state. Likewise a Local Government CIO would be responsible for all city IT issues and would report directly to the Mayor. Overall, the CIO is the chief architect for planning, coordinating, managing and implementing state IT enterprise strategies and architectures. Most importantly, a CIO ensures security is built-in instead of bolted on to any critical infrastructure system.

Currently, more than twenty-five states have cabinet-level CIOs who report directly to their governors [107]. The remaining states currently have CIOs assigned to various departments: administration, personnel, management and budget, and finance.

States with cabinet-level CIOs have distinct advantages. Unfettered access to the states highest elected official. Cabinet level positions also allow larger approval authority for budget outlays. Moreover, cabinet-level positions allow direct control over the IT planning and budget allocations of many departments. Cabinet-level CIOs carry the clout of the Governor's office, which allows them to make prudent IT demands and shut down agencies that do not follow state enterprise architecture strategies.

States without cabinet-level CIOs are at a distinct disadvantage. Access to senior level leadership can be limited. Without cabinet-level authority, there is usually little

control over budget outlays and daily expenditures. By being assigned to a specific director, for example the department of personnel, direct control of other departments who might build their own networks is hindered. Perhaps the largest challenge for non-cabinet level IT positions is that they can be understaffed and dual or triple hatted, working many different jobs. Delaware's Lieutenant Governor articulated that in this environment state employees could not improve the IT structure for the state, it often took weeks to get basic services and IT department employees, who could not control their fate, often viewed themselves as "the dregs of state government" [67].

State and local level CIOs have a demanding task. On a given day there may be 300 or more vendors contacting different state and local departments to compete for contracts and services. A cabinet level CIO ensures that technology applications and critical infrastructure protection decisions are not left to individual state and local departments, thereby preventing duplicative services and expenditures. State and local agencies in difficult economic times cannot afford such waste. Cabinet-level CIOs alleviate this IT island mentality and ensure standardization, economies of scale, interoperability and security through the use of a centralized critical infrastructure protection architecture. Some CIO policies and functions should include: building in security through centralized support services [57]; Standardizing statewide technology policies and equipment purchases in order to deliver high quality—cost efficient services. Furthermore, centralized IT budgeting and expenditure tracking can enhance E-government strategies and deployment methods at the state and local level.

Like the private sector, the public sector must do a better job of understanding the true costs of its systems and protection efforts [57]. State and local CIOs are a critical

link to their private sector and federal counterparts. Without state and local CIOs, industry and the federal government must work with a multitude of agencies and organizations whose individual actions often inhibit an enterprise approach to cyber security. The benefits of having cabinet-level state and local CIOs are seen through sound policy initiatives, which produce fiscal efficiencies, interoperable systems and increased security for state and local critical infrastructures.

CHAPTER VIII

WORKFORCE ISSUES

When medieval castles were attacked, they relied on a mutually supportive combination of defensive structures to achieve maximum protection. Technology, legislation and policy can create the moat, walls and keep for critical infrastructure protection. But for any defensive architecture to work, castle defenders are also needed.

The private sector and state and local agencies would turn to different entities to assist with their critical infrastructure protection needs. For example, the private sector might look to state or federal programs to educate their workforce or to tax incentives to help defray education and training costs. State governments might examine the use of the National Guard to protect networks. Local agencies could consider soliciting volunteers from within their communities. This chapter focuses on engaging corporate employees, state and local agency personnel, volunteers and the National Guard in critical infrastructure protection. It concludes with an analysis of the challenges to information sharing between workforce entities.

8.1 Corporate Employees

Engaging the corporate workforce in critical infrastructure protection is crucial as approximately eighty-five percent of all infrastructures are owned and operated by the private sector. Private sector employees are intimately familiar with their systems and networks, which makes them best suited to performing cyber security tasks. Moreover,

private sector employees are commonly affiliated with Information Sharing and Analysis Centers (ISACs) and can share information with workforce members across all critical infrastructure sectors.

It is well established that enterprises should have one cyber security expert for every ten IT employees. However, most companies have ratios approaching 1:30; some enterprises have ratios as high as 1:300. One problem is that enterprises have no way of knowing if investments in cyber security will generate additional revenue. Furthermore, due to the intangible nature of cyber attacks, it is extremely difficult for enterprises to accurately estimate risk. As a result, most enterprises adopt the mentality that if a major catastrophe strikes, they will be either be bailed out by insurance or government, or simply cease to exist.

Ultimately, fielding sufficient numbers of well-trained cyber security personnel is the most effective way of protecting private sector infrastructures. Since it is always difficult to create new security professional positions, private sector entities would be more inclined to train members of their IT workforce to perform security functions. Thus, federal, state and local agencies should focus on enhancing cyber security education and training opportunities. Special grants could be provided to state universities, community colleges and career and technology education centers to offer education and training programs designed specifically for the workforce. Likewise, scholarships and grants could be made available to members of the workforce to enable them to pursue degreed and non-degreed educational programs. Finally, tax incentives could be provided to corporations to encourage them to offer in-house or offsite cyber security training for their IT employees.

8.2 State and Local Agency Personnel

State and local agency employees are best suited to protect their own electronic assets. Unfortunately, due to consistent budget cuts over the past several years, most agencies have insufficient IT personnel to conduct normal operations, let alone perform security related activities. Moreover, these agencies have huge shortages of trained cyber security professionals. Indeed, the cyber security workforce situation at state and local agencies is far worse than that in the private sector.

The best solution, once again, is to train members of the IT workforce to perform cyber security functions. Fortunately, state and local governments have more leeway in ensuring that their employees receive education and training opportunities. Many public education institutions, e.g., state universities, community colleges and career and technology education centers, have special academic and training programs for state and local employees, especially in areas related to homeland security. Such programs could be broadened to offer cyber security curricula. State and local agencies could encourage their employees to avail of these and other cyber security education and training opportunities, possibly by providing scholarships and offering flexible work hours and school leave incentives.

8.3 Volunteers

Using a volunteer force is another option for critical infrastructure protection. There are potentially large numbers of volunteers to fill the vacant roles for state and local cyber defense needs. Since September 11, 2001, many Americans are rethinking their career choices, and increasing numbers are being drawn to service careers such as

law enforcement, emergency services, education and the military. The Bureau of Labor Statistics reports that 59.8 million people did volunteer work in 2002, which increased to 63.8 million in 2003. In 2004, more than 28.8 percent of Americans served as volunteers [98]. As in the 1940's, there is the potential for a national movement of volunteers to support government efforts—especially at the state and local level. In the 1940's, President Franklin D. Roosevelt's administration called for an engaged citizenry whose volunteer efforts made them the "greatest generation." Another volunteer force is being created under the umbrella of the USA Freedom Corps. This volunteer program allows individuals to become involved in the war against terrorism by making America's homes, neighborhoods, schools and workplaces safer. The FBI's InfraGard program is another way citizens can work within their communities to help protect America's critical infrastructures [36].

However there are many obstacles to using volunteers. Volunteer forces may not be familiar with the technical aspects of the systems they could be required to manage. Lack of training can result in trust issues with enterprise owners. Also, training presents a problem, as it is likely to be non-standardized and unscheduled over the lifetime of projects, which could result in serious liability issues. Moreover, in the area of critical infrastructure protection, volunteers tend to have a horizontal focus looking across many sectors such as power, telecommunications and information technologies, but have very limited vertical focus because of the issues described above. Finally, many individuals may not wish to volunteer their time at a keyboard. Unlike traditional public service activities, which are both rewarding and inspiring, performing computer security tasks can be a thankless pressure-packed job.

8.4 National Guard

The National Guard, at first glance, is an attractive option for statewide critical infrastructure protection. It is well funded, well organized and has a significant presence in every state. In addition, the Guard provides regional and national interoperability (e.g., its training and systems are standardized). Many Guard members either have the expertise or can be trained to support critical infrastructure protection efforts. Furthermore, Guard members often possess security clearances that enable them to access classified information.

However, engaging the National Guard in critical infrastructure protection poses several challenges. The most significant is that during times of international crises, the National Guard, because of U.S. Code Title 10, is subject to being recalled to active duty status. As such, there may only be small numbers of guardsmen available to perform state level missions. In February 2004 many of the nation's governors expressed great concern about the increasing demands placed on National Guard units [80]. As of February 2004, the Guard constituted about twenty-two percent of the forces in Iraq; this number is expected to rise (along with the National Reserves) to nearly forty percent as a result of force rotations [80]. Another challenge to engaging the National Guard is the functional limitation placed by Title 10. When operating under this statute, the Guard is constrained by the *Posse Comitatus Act* of 1878, which precludes the use of the military in situations where civilian forces could serve. Moreover, the Guard has retained a traditional focus within the Department of Defense, concentrating on military field exercises and preparations for real world deployments as opposed to critical infrastructure protection. Finally, due to network uniqueness and liability issues, CIOs

and executive management would be unwilling to grant outsiders access rights to their systems and networks, membership in the National Guard notwithstanding.

8.5 Information Sharing

Despite technologies, legislation and policies to improve information sharing, federal agencies, state and local governments and the private sector generally do not consider current information and intelligence sharing approaches to be effective. According to a 2003 GAO survey, fewer than 60 percent of federal, state and local respondents rated the current sharing process as effective or very effective [100]. The Major Cities' Chiefs Association has emphasized that the federal government must better utilize and integrate the nation's local law enforcement officers into the information sharing process [50]. The National Governors Association has stressed that "law enforcement and public safety agencies do not always have access to timely, complete and accurate information" [100]. Additionally, the International Association of Chiefs of Police testified before the U.S. Senate Committee on Governmental Affairs in 2002 that information sharing was not effective because there are no existing policies to fully integrate state and city workforce members into the national intelligence process [100]. Because fighting terrorism is considered to be a federal responsibility, the federal government generally has not shared intelligence with state and local agency personnel. The result is constrained information flow compounded by federal policies that do not support the granting of security clearances to state and local officials, denying them access to vital classified information [100].

Some of these views and policies stem from the 1940's when the federal government began to separate law enforcement and intelligence functions. Few individuals outside the military and intelligence communities had clearances to access sensitive information [100]. The granting of security clearances to state and local government officials was also limited by the *1978 Foreign Intelligence Surveillance Act.*

In 2001, Congress attempted to remedy this situation by passing the *USA PATRIOT Act.* The *PATRIOT Act* provides federal investigators with greater flexibility in sharing information obtained under the *1978 Foreign Intelligence Surveillance Act* [100]. The subsequent *Homeland Security Information Sharing Act* of 2002 mandates the sharing of homeland security information between federal, state and local agencies; in particular, it provides for the sharing of classified information and sensitive (unclassified) information [100]. State and local agency personnel may not access classified information unless they possess the proper clearances as directed by *Executive Order 12968. Executive Order 12968 (Access to Classified Information)* stipulates that access to classified information is generally limited to persons: possessing security clearances, who have been trained in the handling and protection of classified materials and who have signed documentation agreeing to abide by all the appropriate security requirements in support of the nation's defense [100]. As a result, the issue arises of how to pass actionable intelligence to state, local and private sector personnel who do not possess the proper clearances. For example, without such intelligence information, local law enforcement personnel would not be able to connect information gathered from simple events (e.g., traffic violations) and place them in the larger context of terrorism investigations [100].

The *2002 Gilmore Commission* reflected the view that the federal government likes to receive information but is reluctant to share information with its homeland security partners [100]. One solution is to designate "trusted agents" at state and local entities and their private sector partners, who would receive clearances. Concerns about the ability of these individuals to properly handle classified information are mitigated by the fact all these entities have procedures in place to deal with sensitive information. For example, state and local law enforcement agents already handle sensitive forensic information; with proper training they could also handle classified information [100]. Meanwhile, the Department of Homeland Security is weaving technology (e.g., secure telephones to all governor's offices) and policy (e.g., security clearances to key state and local government entities) so that vital information can be shared in accordance with prevailing laws [21].

While these efforts are promising, certain cultural barriers have yet to be overcome. For example, security clearances issued to individuals by one federal agency are often not recognized by other agencies. One promising solution is contained within the *Homeland Security Information Sharing Act,* which recognizes that the sharing of information is much more effective when it is unclassified. Intelligence information that is collected can be stripped of its sensitive sources and collection methods, and then transmitted to state and local agencies. This "cut-line" information (i.e., stripped of sources and methods) can be transmitted using the National Law Enforcement Telecommunications System and the Regional Information Sharing Systems, which already reach 18,000 law enforcement agencies across the United States [33].

CHAPTER IX

RECOMMENDATIONS FOR STATE AND LOCAL ENTITIES

State and local agencies must be actively engaged in homeland security and critical infrastructure protection efforts. Recognizing their vital role, former Oklahoma Governor Frank Keating noted: "It is important for the nation's governors to focus on what can be done at the local level to prepare for and respond to all forms of attack" [62].

In order to be successful in critical infrastructure protection and cyber security efforts, state and local governments must participate in regional partnerships, expand education and training programs, create centers of excellence, establish an IT emergency services network, improve information sharing, weave technology, legislation and policy, and effectively link state and federal programs. This chapter discusses each recommendation in detail.

9.1 Regional Cooperation

Efficient and cost effective regional defense constructs are essential. Even with the federal increase in homeland security spending, the nation—much less individual states—cannot afford the cost of new organizations and programs that exist solely to prevent or mitigate attacks. This is particularly evident when taking into account the fact that a terrorist event has a low probability of occurrence. Moreover, it is politically

difficult to move funding from other important programs to support infrastructure protection efforts.

In Oklahoma, for example, the lack of funding for schools and prisons has reached crisis proportions, making it difficult to fund security programs. In 2003, Kentucky's fiscal situation grew so dire that the governor authorized the release of criminals from prisons before their sentences were complete. Moreover, in 2003, the head of Kentucky's Public Advocacy Department warned that if his office's budget were cut again, his lawyers to would have to refuse all *pro bono* cases even though Kentucky is required by its Constitution to provide criminal defense attorneys to all individuals who cannot afford them. Against this backdrop, state and local governments struggle to obtain funding for their most urgent critical infrastructure protection initiatives [46].

Given this situation, it is appropriate for states to look to one another for support. Regional collaboration efforts among states will strengthen the overall security posture of each state and its partner states while collectively easing the financial burden.

Regional cooperation among states is a clever solution to a problem inherent in federalism. Due to concerns about federal tyranny, it is unlikely that the citizenry would support transfer of traditional state and local responsibilities to the federal government. Yet individual states and local agencies, whether from budget crises, lack of expertise or a host of other limitations, cannot handle all homeland security and critical infrastructure protection functions on their own. Regional programs have the advantage of reducing the competition for federal money. Indeed, interstate compacts have long been used to address environmental policy, law enforcement, economic development and other issues.

Homeland security and critical infrastructure protection are a natural fit for such cooperative approaches.

In addition to regional cooperation between states, partnerships should be developed between states and the Department of Homeland Security to coordinate infrastructure protection and emergency response efforts. These include joint protocols for operational entities and senior decision-makers in state and local governments, the federal government and the private sector. Some of the most promising collaborative efforts to date include [104]:

- U.S. Attorneys for judicial districts working with the FBI to enhance coordination and information sharing with state and local governments through Anti-Terrorism Task Forces and Joint Terrorism Task Forces.

- States working in partnership to develop virtual joint information systems to respond to major emergencies.

It may not be possible to locate an information center for critical infrastructure protection in every state. However, it is feasible to operate virtual joint information centers that would serve regional needs, especially sharing infrastructure security related information between the various stake holders, and communicating information about threats and response strategies to the media and the general public.

9.2 Cyber Security Education and Training

Cyber security education and training and associated workforce development programs are by far the quickest and the least expensive of all investments in critical

infrastructure protection. Moreover, they offer the greatest potential return. By educating both the current workforce as well as the next generation of cyber security professionals, state and local governments can achieve a critical mass of technical proficiency in their IT workforce.

Responding to future threats—whether they are cyber, biological or chemical—will require the development of new programs and the refinement of existing curricula. America's colleges and universities offer an immediate opportunity to design and deliver academic opportunities—saving time, money and potentially human lives.

Education and training programs must focus on the existing workforce as well as the next generation of cyber security professionals. Oklahoma's CareerTech System, which is representative of vocational education systems in most states, offers programs and services in 29 technology center districts operating on 54 campuses located in 400 comprehensive school districts, and also includes 25 skill centers [63]. Clearly, vocation education systems like Oklahoma CareerTech are ideal vehicles for providing traditional as well as distance learning programs across states.

Another attractive educational initiative is to create a "Cyber Corps Program" for state and local agencies that is patterned after the highly successful federal initiative. The federal Cyber Corps Program, which incorporates the NSF Scholarship for Service (SFS) Program and the Department of Defense Information Assurance Scholarship Program (IASP), was launched by Presidential order in December 2000 to create a cadre of highly trained information assurance professionals for the federal government and military. The program offers two-year scholarships to high-achieving undergraduate and graduate

students in computer science and related fields. Cyber Corps students undergo an intense regimen of coursework, research and capstone projects in information assurance, coupled with a summer internship at a federal agency. Upon completion of their programs of study, Cyber Corps students are required to serve in the public sector for at least two years. Since the fall of 2001, the Cyber Corps Program has grown to include in excess of thirty colleges and universities from across the country, and has produced more than 300 elite information assurance professionals for the federal government and military.

A state and local Cyber Corps program would parallel the federal effort, except that it would engage two-year academic institutions (e.g., community colleges and vocational technical centers) as well as four-year and graduate universities to build a cyber security workforce for state and local agencies. Students pursuing undergraduate and graduate degrees specializing in information assurance would receive two-year scholarships and a paid summer internship in return for serving for at least two years with a state or local agency. Students from two-year institutions would receive one-year scholarships that would support the A.S. or A.A.S degree studies. Thereafter, they could either serve with a state or local agency, or continue to receive their scholarships while they pursue their baccalaureate degrees at an accredited university within the state. In all cases, students would be required to serve as information assurance professionals with state or local agencies for at least one year for every year of scholarship assistance received.

Funding for this most innovative program could come from the National Science Foundation (NSF), which is already supporting cyber security workforce development programs (e.g., Advance Technological Education (ATE) Centers) across the country. In addition, state legislatures and municipalities could leverage funds already allocated for

academic and scholarship programs at community colleges and vocational technical education centers to institute successful state and local Cyber Corps programs.

9.3 Centers of Excellence

The Department of Homeland Security has been designated as the federal center of excellence for cyber security and critical infrastructure protection. Likewise, equivalent agencies in state and local governments should be designated as centers of excellence that would spearhead infrastructure protection efforts in their jurisdictions. Specifically, state and local governments should [105]:

- **Establish Rapid Identification and Information Exchange** between all critical infrastructure stakeholders by creating state and local ISACs.
- **Ensure Federal Actions to Secure Cyberspace are Directed at State and Local Entities** in order to effectively reach the nation's populace and the private sector through joint policy efforts.
- **Establish State and Local Centers of Excellence** to foster partnerships between government and industry and provide joint analysis issuance of warnings and computer emergency response.
- **Establish Cyber Security Planning** to assist small businesses and non-governmental agencies with incident response and disaster recovery efforts.
- **Establish Watch–and–Warning Networks** in state and local jurisdictions to rapidly disseminate information about risks, vulnerabilities, threats and attacks.

- **Enhance Cyber Threat Analysis** to address long-term issues related to risks, vulnerabilities, threats and attacks through partnerships with federal and private sector entities.

9.4 IT Emergency Services Network

It is vitally important that each state adopt a single incident command system using its statewide network as the transport layer. Any degree of disorganization or confusion resulting from inadequate command and control is only exacerbated in times of emergencies [28]. During the September 11 attacks on the Pentagon, telephone networks in Washington D.C., Virginia and Maryland became saturated as calls from concerned citizens spiked. In this particular scenario, critical communication services for the state could have been "failed over" to a Voice over IP (VoIP) solution on the state's networks, helping to maintain vital emergency communications services.

In addition to voice networks, many states operate sensors that are placed on towers located throughout the states. The State of Oklahoma, for example, maintains forty-seven towers with Doppler radar sensors on them. While their primary mission is to track tornados and other severe weather events, these towers can be used for other purposes such as detecting radiological, chemical and biological agents.

State and local networks offer significant connectivity and bandwidth to support public services such as distance learning and telemedicine. This connectivity and bandwidth could be used to support emergency operations. National Guard units could also install their command centers in almost any municipality and utilize state and local network resources. For example, Oklahoma's OneNet has forty-two hub sites with T-1

or higher connectivity located in almost every local community. A formal plan for law enforcement, medical personnel and the National Guard to use this resource will enhance on-site operations as well as save lives.

By utilizing statewide networks, communication interoperability is significantly enhanced through the standardization of systems. Furthermore, statewide networks can support the continuity of critical government operations. Consider the anthrax attack on the Hart Building in Washington D.C., which forced an evacuation of all government workers for three months. If a similar attack had been perpetrated on a State Capitol, the Governor would have to ensure that the government could still operate. By moving to a designated site close to the capitol, video teleconferencing could be conducted with all municipalities in the state. Furthermore, mobile command and control, medical support, communication interoperability, access to experts and uniform incident command all can be supported by statewide network backbones, enhancing the response to terrorist attacks as well as natural disasters.

9.5 Information Sharing

Information sharing is a cornerstone for developing comprehensive and practical strategies to defending critical infrastructures against cyber and physical attacks. Information sharing needs to be streamlined both within the government and between the public and private sectors. The development of state and local level Information Sharing and Analysis Centers (ISACs) would bridge the gap between government and industry at the local level, providing for meaningful dialogue and increased security. State and local ISAC efforts involve [99]:

- **Establishing Trust Relationships** with federal and non-federal entities to provide information and advice on vulnerabilities and incidents through scheduled meetings, exercises and "off-sites" for team building purposes.
- **Establishing Secure Communications and Networks** between state and local entities, the federal government and the private sector through the use of secure telephones and shared networks.
- **Establishing Standards and Agreements** for sharing information and protecting it from unauthorized disclosure.

Developing standards and agreements for sharing information is a particularly thorny issue. One challenge to information sharing is the reluctance of the private sector to participate in traditional ISACs due to concerns about the release of sensitive information under the *Freedom of Information Act (FOIA)* [9]. Under current FOIA provisions, there is the presumption that records in the possession of agencies and departments of the U.S. government are accessible to the public. Recognizing the legitimate need to restrict disclosure of some information and to promote the cooperation with statutes and regulations, the federal government has provided exemptions under which information need not be disclosed [65]. The *Davis-Moran Act,* for example, affords a certain degree of protection from FOIA requests to companies that voluntarily provide information to the government. L. Craig Johnstone of the U.S. Chamber of Commerce echoed the fears of industry on public disclosure and praised Congress's efforts in this area: "the government can expect the amount of valuable information passed on to agencies about Internet threats and vulnerabilities to be directly proportional to the amount of safety provided by the *Davis-Moran Act*" [65].

In addition to increasing security, state and local ISACs can tighten and promote public-private sector partnerships. The FBI's InfraGard Program serves as a model for establishing state and local ISACs; it has representation from industry, government agencies, state and local law enforcement, and the academic community. Such programs act as clearinghouses for information exchange, and helps to consolidate efforts between the private and public sectors. They also streamline information flows between federal agencies and state and local entities [100].

9.6 Weaving Technology, Legislation and Policy

Defending state and local critical infrastructures requires a mutually supportive combination of technological, legislative and policy initiatives. Isolated solutions will not produce the synergy needed for adequate defense. Like the defenses in medieval castles, technology, legislation and policy must be strategically woven to protect critical infrastructures.

9.6.1 Defense in Depth Elements

The key elements of defense in depth for critical infrastructure protection are technology, legislation and policy. The technological element, as outlined in Chapter V, comprises automated systems for real-time monitoring, data collection, and analysis. Also, it incorporates hardware, software, physical security and human access controls that provide enterprise security. All of these measures should support each other to effectively secure critical infrastructure components. The legislative element, outlined in Chapter VI, comprises statutes such as the *Computer Fraud and Abuse Act*, the *Electronic Communications Privacy Act* and the *USA PATRIOT Act*. These statutes and

others protect electronic assets as well as the rights of individuals. The policy element, outlined in Chapter VII, articulates what must be protected and how resources are to be allocated and used. Policy sets the priorities and the agenda for entities involved in critical infrastructure protection. Combining all three elements yields a mutually supportive approach to critical infrastructure protection, much like the interlocking walls, moat and keep of a medieval castle system.

9.6.2 Mutually Supportive Approach

The mutually supportive approach of weaving technology, legislation and policy underlies recent Congressional legislation on information security practices. The legislation is effective because it captures and articulates sound policy, which drives appropriate technological solutions. The *Government Information Security Reform Act* (GISRA) and the *Federal Information Security Management Act* (FISMA) are examples of this synergy. GISRA established information security certification programs, independent evaluations and reporting requirements for the federal government. FISMA strengthened and permanently authorized both GISRA and the *Homeland Security Act of 2002*. Both acts helped consolidate essential critical infrastructure protection functions and agencies into the Department of Homeland Security. In addition, the legislative efforts have positively impacted the administration, certification and secure operation of critical infrastructure networks. Indeed, technological, legislative and policy actions have been aligned and woven, contributing significantly to the nation's critical infrastructure protection posture.

Unfortunately, scenarios abound in which the alignment and weaving of technology, legislation and policy do not occur. For example, in *Kyllo v. United States*, the Supreme Court ruled that the warrantless use of a thermal imager on a suspect's home during a search violated the Fourth Amendment. The court held that when law enforcement "uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without a physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant" [97]. The *Kyllo* case underscores the need to align technology, legislation and policy. The misalignment resulted in a use of technology that violated constitutional law and ultimately undermined the prosecutions efforts.

In summary, state and local governments must integrate the mutually supportive elements of technology, legislation and policy in their critical infrastructure protection efforts. Such coordinated efforts will result in broader, more robust and less expensive protection of critical infrastructure assets.

9.7 Federal Programs

State and local governments can indeed create a seamless web of security for citizens. But they will require more from the federal government than a policy publication like the *National Strategy to Secure Cyberspace*. Lt. Gov. Dave Heineman of Nebraska said budget realities prevent direct responses to threat warnings. "We can't afford not to take it seriously," he said, "but on the other hand, that doesn't mean we run out and put 50 additional law enforcement personnel on the street either" [5]. How much federal funding state and local agencies receive and how they utilize this funding will, in

large measure, dictate their success in providing homeland security and critical infrastructure protection for their constituents.

The pursuit of funding by state and local entities should follow a commitment to action that architects programs. State and local cooperation and responsibility should be measured in terms of reporting on efforts and accomplishments. Reporting is an effective tool for perception management and building up public confidence. Without a reporting structure, federal, state and local agencies cannot assess the risks, vulnerabilities or even the viability of critical infrastructure programs. Anthony Cordesman of the Center for Strategic and International Studies has maintained, "if the federal government needs auditing and effectiveness measures, so do state and local governments" [13].

"Protecting the health and safety of our citizens is a responsibility that weighs heavily on governors," said former Utah Governor and co-chair of National Governors Association's Homeland Security Task Force, Mike Leavitt. "The National Governors Association and the Homeland Security Task Force are dedicated to working with local and federal government—and the private sector—to continue to address the complex challenges of protecting America from terrorist threats both foreign and domestic" [13]. In order to prepare for possible critical infrastructure attacks, the National Governors Association has made several major recommendations [3]. These recommendations support the priorities and issues identified by state and territorial officials across the country [2].

- Coordination must involve all levels of government.
- The federal government must disseminate timely intelligence information to states.

- States must work with local governments to develop interoperable communications between first responders and adequate wireless spectrum must be set aside to accomplish the task.
- State and local governments need help and technical assistance to identify and protect critical infrastructures.
- The federal government should provide adequate federal funding and support to ensure that state and local homeland security needs are met.
- The federal government should work with states to protect sensitive security information, including restricting access to information available through "freedom of information" requests.
- The National Guard has proven itself to be an effective force during emergencies and crises. The mission of the National Guard should remain flexible, and Guard units should primarily remain under the control of the governor during times of crises.

The recommendations made by the National Govoners Association involve cooperation between federal, state and local agencies in homeland security and critical infrastructure protection. But just as important is federal support for state and local initiatives.

Due to tight state and local budgets, important issues such as homeland security and critical infrastructure protection are being passed over in favor of other more prosaic public services. Other statutory limitations exist as well. In Oklahoma, for example, State Question 640 (which requires any revenue raising measure to have 75 percent approval of the state house and senate) has made it difficult to generate new tax revenue. Without federal support, many state and local level homeland security and critical

infrastructure protection efforts will likely fail. The federal government must provide stable funding for state and local entities. At the same time, it must ensure that the monies are spent wisely on securing the homeland.

CHAPTER X

ECONOMIC SUPPORT FOR CRITICAL INFRASTRUCTURE PROTECTION

Steady funding is vital to critical infrastructure protection. This chapter discusses the distribution of responsibilities for costs among federal, state and local government entities. It also explores the economic basis for government intervention.

10.1 Costs to State and Local Governments

The task of securing critical infrastructures requires substantial funding. However, state and local budgets are under increasing pressure, and CIOs continue to significantly reduce budget outlays while attempting to maintain service levels. At this time, state and local governments are confronting their worst fiscal crisis in half a century. Many state IT budgets took big cuts in 2003. The National Conference of State Legislatures reported that states are faced a $68.5 billion budget shortfall for FY04 [53]. In an economic downturn, the demand for services increases, creating a troubling paradox. More citizens file for unemployment and other benefits, which means that state and local systems experience growth. Keeping the infrastructure running becomes essential. But reduced funding for IT infrastructures leads to lower service levels for citizens and agencies [46].

The 2004 U.S. Conference of Mayors Report presented the results of a survey of 150 cities with populations ranging from 30,000 to eight million. The survey found that cities were spending nearly $70 million per week in additional homeland security costs

due to contingencies abroad and heightened threat levels. If the war and/or threat levels continue for six months, the cities would incur nearly $2 billion in additional costs on top of existing homeland security spending [92].

State and local governments realize how dependent their operations are on information technology. As a result, CIOs have begun to examine the impact of cuts or cost-containment measures on their infrastructures and on their ability to deliver services to citizens [46]. Budget cuts that result in scaling back IT operations from 24/7 to business hours severely limit access to public services. For example, public safety could be degraded if a law enforcement officer could not electronically process a wanted persons inquiry because budgetary constraints affected the availability of the appropriate databases [46].

10.2 Market Failure as a Rationale For Government Intervention

According to Tom Ridge, Secretary of the Department of Homeland Security, the "miracle of the marketplace" will not necessarily solve all the problems related to securing the nation [103]. If the nation's market system were carried out to perfection, private sector motivation through the operation of markets ought to be sufficient to provide optimal protection for society as a whole. But why doesn't the market provide for security? The answer lies at the heart of most any economic rationale for public policy—market failure. Market failure occurs when the behavior of agents in the market fail to bring about the efficient allocation of some good [8]. Such failures often spur government intervention in the name of public interest.

Many national security endeavors require government action (e.g., intelligence gathering, national defense and border security). In the case of some other endeavors, incentives exist for the private sector to provide security. For example, corporations that rely upon the Internet to conduct business have the motivation to provide a satisfactory level of security against denial-of-service (DoS) and other cyber attacks on their servers.

According to the *National Strategy for Homeland Security*, "the government should only address those activities that the market does not adequately provide" [88]. A Brookings Institution publication, *Protecting the American Homeland*, offers justifications for such government intervention [59]. Although its justifications are by no means exhaustive, the publication argues that homeland security and critical infrastructure protection may be motivated by nearly all types of market failure. Six key market failure examples associated with homeland security are discussed below. These examples provide the rationale and justification for government action.

Homeland security and critical infrastructure protection can be viewed as "public goods." Public goods are, to varying degrees, nonrivalrous in consumption, non-excludable in use, or both [106]. Public goods and services provide benefits to multiple individuals at a time, and their use cannot be restricted to only those individuals who have paid to use them. If a good or service cannot be withheld from those who do not pay for it, providers expect to be unable to sell it and, therefore, will not produce it. In market economies such as the United States, federal, state and local government often provide these goods and services, or they would not otherwise be offered.

Inherent to the nature of homeland security as a public good is the so-called "free rider problem." Allocative efficiency in the provision of pure public goods occurs when the sum of individual marginal utilities equals the marginal cost of provision. The free rider problem arises when there is a strong incentive for individuals to misrepresent their true marginal utilities for public goods. Thus, free riders receive the benefits of public goods without helping cover the costs of producing those benefits.

In the case of homeland security and critical infrastructure protection, the free rider problem is perhaps most evident in the unwillingness of citizens to pay more taxes. Most citizens agree that they want more homeland security (or for that matter more government services), but few are willing to pay more through taxes or other measures. The free rider problem is a major reason why private markets do a poor job of supplying public goods such as critical infrastructure protection.

Just as apparent as the free rider problem is the view of terrorism as a negative externality. A negative externality is an uncompensated harm resulting from any action that affects an unconsenting population [106]. The canonical example of a negative externality is environmental pollution generated by industrial plants.

When dealing with terrorism, negative externalities arise in the security measures implemented prior to an attack and in the consequences of an actual attack. The most obvious negative externalities associated with terrorism are the costs incurred as a result of a terrorist attack, both economic and non-economic. According to the Office of Management and Budget, the financial expenditures directly related to the September 11

attacks were more than $100 billion. The non-economic costs include injury, death as well as reduced consumer confidence and an increasingly concerned citizenry.

Other negative externalities arise when systems and facilities are used as instruments of terrorism. For example, loose security on corporate servers might provide terrorists with platforms for launching cyber attacks. In such a scenario, the costs resulting from the attacks would not be shouldered by the corporations. This negative externality serves as the basis for government intervention to secure critical computer systems and facilities, which hinges on private markets' underinvestment in antiterrorism measures. Individuals or firms will often decide how to protect themselves against terrorism without considering fully the external costs of an attack. Therefore, governmental involvement (e.g., threat of regulation), especially at the state and local levels, is necessitated to ensure satisfactory investments in security.[3]

In the critical infrastructure protection realm, negative externalities also manifest themselves through the reluctance of enterprises to report security breaches in their infrastructures, because the costs of reporting often exceed the losses from a breach. Enterprises struck by Internet attacks that cause relatively small financial losses may choose to absorb the losses in the hopes of keeping the incident a secret. The potential harm to the enterprises' reputations due to the negative publicity from an incident would probably outweigh the financial losses due to the incident. The tendency of corporations

---

[3] An interesting footnote from *Protecting the American Homeland*: "The Coase theorem shows that under very restrictive conditions, the negative externality can be corrected by voluntary private actions even if the role of government is limited to enforcing property rights. But the Coase theorem requires that all affected parties be able to negotiate at sufficiently low cost with each other. Since virtually the entire nation could be affected indirectly by a terrorist attack, the costs of negotiation are prohibitive, making the Coase theorem essentially irrelevant in the terrorism context" [106].

not to share information about security breaches with other entities, including government agencies, makes it very difficult to assess risk and to compute losses.

"Government intervention can be justified by the cost and difficulty of accurately evaluating security measures" [59]. This is basically a problem resulting from imperfect information. For example, corporations have no way of knowing if IT security expenditures will generate any additional revenue.

Most companies are also uncertain about their exposure to risk due to the intangible nature of cyber attacks. Imperfect information makes it difficult to perform traditional cost-benefit analysis because the associated risk reduction is hard to quantify. This difficulty is also seen in the larger homeland security effort. Corporations choose not to make extra security investments to address levels of risk that often are not understood. Therefore, the government may be justified to set minimum antiterrorism standards through regulatory statutes for IT security given the clear and present danger of terrorist attacks.

Laws themselves can induce market failures. The financial exposure of corporations and individuals to losses from attacks is inherently limited by bankruptcy laws [59]. Therefore, corporations and individuals may not have sufficient motivation to provide an adequate level of security for their systems. Internet start-up companies, for example, may not be motivated enough to invest in security because they can declare bankruptcy and not be held liable for damages in excess of the value of their net assets. The government must address the need to protect against large-scale terrorist attacks in the face of limits to exposure imposed by bankruptcy laws.

In addition, antitrust laws make corporations hesitant to cooperate with other firms within their industry. Due to the potential of antitrust action, some corporations do not engage other corporations to ensure that proper security measures are implemented across their sector. Therefore, government action may be justified in waiving certain antitrust rules that discourage cooperation among competitors. The federal government has developed such guidelines for the health care industry (e.g., HIPAA), but none exist for the IT sector.

A moral hazard arises as a result of the private sector's expectation that the government would bail it out in the event of a significant terrorist attack. As Department of Homeland Security Secretary Tom Ridge put it, "individuals [and the private sector] assume their bill will be sent to Washington" [101]. The $15 billion *Airline Transportation and Systems Stabilization Act* of September 2001 is an example of such a federal bailout. The moral hazard lies in the fact that private individuals' and firms' expectations lead them not to invest in security as they otherwise would. Therefore, if the government cannot credibly convince the private sector that no bailouts will occur after an attack, it may have to intervene before an attack to offset the adverse incentives created by the expectation of bailouts [59].

Finally, incomplete markets may justify government intervention. The most pertinent example is the insurance market. After the September 11 attacks, the insurance industry faced its biggest single loss ever—property, liability, life and workers' compensation claims totaling about $50 billion. The previous record was $34 billion in the aftermath of Hurricane Andrew. These extreme financial burdens often prevent insurance firms from obtaining reinsurance coverage for terrorism risks. The moral

hazard arises once again. Insurees may have a reduced incentive to prevent compensable losses. If fully insured, insurees can make their situation better, and perhaps society (in the aggregate) worse, by spending less of their own resources on loss prevention than they would in the absence of insurance. Therefore, the government may need to step in and help address this problem.

This was exactly the reasoning used on November 14, 2002, when the U.S. House of Representatives adopted legislation providing up to $100 billion to the insurance industry to help cover future terrorist attacks. Under the legislation, the government would pay 90 percent of the cost of a terrorist attack beyond losses of $10 billion. For lesser damages, during the first year of the three-year program, insurance companies would pay up to 7 percent of their premiums for damages with the government picking up the rest of the expenses. By the third year, the insurers' share would rise to 15 percent of their premiums. In that year, the government would pay 90 percent of losses greater than $15 billion [90].

The market failures discussed above represent the most common justifications for government intervention. The relative significance of each factor varies across the different facets of homeland security and critical infrastructure protection. Although it is possible that government intervention may lead to government failure in some actions, there are fundamental economic motivations for policy response. The strength of the U.S. market may be one of the nation's greatest assets as America's demand for innovation increases in the face of terrorist threats. Yet, state and local level government intervention in the name of public interest is warranted in many instances due to market failures.

CHAPTER XI

CONCLUSIONS AND RECOMMENDATIONS

Protecting America's critical infrastructures is a permanent challenge that requires national resolve and continued response. An excellent start has been made through the development of national cyber security policies and laws, and various executive branch initiatives. Although the establishment of the Department of Homeland Security may make it appear that critical infrastructure protection is now a federal responsibility, it is incorrect to assume that state and local governments have anything less than critical roles. Indeed, critical infrastructure protection initiatives will not succeed without the active engagement of state and local governments.

States and local governments, whether from budget crises, lack of expertise or other reasons, cannot handle homeland security and critical infrastructure protection functions alone. Regional cooperation has the distinct advantage of reducing the competition for federal funding between state and local agencies and has the added benefit of integrating the private sector, which owns and operates a full eighty-five percent of America's critical infrastructure assets. Moreover, coordination between state and local government agencies and private sector entities can help alleviate interoperability issues.

By effectively linking state and local programs to federal and private sector initiatives, a new breed of federalism can be implemented: one that involves state and local entities during periods of peace and prosperity and during times of tension and

crisis. To assist in this effort, joint policymaking and funding initiatives should be enacted. Furthermore, regional alliances will help create sound, cost-effective defensive postures, enabling state and local partners to achieve the "Oklahoma Standard."[4]

Information sharing underlies all critical infrastructure protection efforts. Improved communications and information sharing can be accomplished through the establishment of state and local Information Sharing and Analysis Centers (ISACs). These ISACs will help bridge the gap between government and industry at the regional, state and local levels and provide increased security. Information sharing also facilitates interoperability between organizations and systems.

A well-trained workforce is needed to implement critical infrastructure protection efforts. A Cyber Corps Program [8] modeled after the federal initiative could help produce cyber security professionals for state and local agencies. Similar programs could be instituted to enhance expertise in the private sector.

The strategic weaving of technology, legislation and policy clearly enhances the ability of state and local governments to provide critical infrastructure protection. By aligning the "threads" of technology, legislation and policy, the strength in the fabric of state and local critical infrastructures can be maximized. Future research efforts should focus on the following areas:

---

[4] Oklahoma is recognized as a national model for disaster response, having received wide attention for its efficient, coordinated response to the Alfred A. Murrah Federal Building bombing. Continuing to learn and build on that experience, state and local agencies have worked together to hone first responder procedures and policies. Prevention is a priority as well. To that end, state, local and federal law enforcement agencies in Oklahoma have established communication protocols and strategies to build a premier state intelligence network. These efforts have become known as the "Oklahoma Standard" [83].

- **Technology**: Design processes for centralized purchasing of technology hardware, software and human services between federal, state, local and private sector entities. By making centralized purchases, millions of dollars can be saved. Moreover, interoperability between state and local entities and federal agencies can be enhanced through preferred product listings and "group" purchasing.

- **Legislation**: Design models for regional cooperation between state and local entities that center on the 94 U.S. judicial districts that are organized into 12 regional circuits. Such a model would also facilitate the uniform treatment of legal issues that currently vary across the 87,000 jurisdictions within the United States.

- **Policy**: Identify why the disbursement of federal homeland security and critical infrastructure aid to state and local entities has been slow. Design a model for centralized homeland security grant processing that focuses on regional needs vice individual grants.

Asking the right questions regarding critical infrastructure protection at the state and local level is also extremely important. Who better than state and local governments to provide the stability needed for sustained critical infrastructure protection efforts? And who better than state and local governments to work with America's industries that are located within their borders?

The time is ripe for a new model that recognizes the importance of state and local governments in defending the homeland. By weaving technology, legislation and policy, a defense in depth architecture can be formed, enabling state and local communities to

cut the Gordian knot[5] of cyber security and successfully protect America's critical infrastructures.

[5] Legend has it that after Alexander the Great led his army into Asia Minor; he went to worship in the temple of Zeus in the city of Gordium. In the temple there was a wagon, which had formerly belonged to Midas, King of Phrygia. It was secured very tightly by a knotted cord, that no one had been able to untie. Faced with this, Alexander pondered for a moment, drew his sword and severed the knot with a single stroke [81].

BIBLIOGRAPHY

[1] Alberts, A., Garstka J. and Stein, F. (2000) *Network Centric Warfare: Developing and Leveraging Information Superiority 2nd Edition.* CCRP Publication Series (www.ccrp.com).

[2] Beauchesne, A. (2001) *Homeland Security: The Cost to States for Ensuring Public Health and Safety*. National Governors Association (www.nga.org).

[3] Beauchesne, A. (2002) *States' Homeland Security Priorities*. Issue Brief, NGA Center for Best Practices (www.mwsc.edu).

[4] Branscomb, A. (1990) Rogue computer programs and computer rogues: Tailoring the punishment to fit the crime. *Rutgers Computer & Technical Legal Journal*, **16 (1)**.

[5] Bumiller, E. (2002, November 16) Terror alert brings new steps to prevent attacks, U.S. says. *The New York Times*, New York.

[6] Carpenter, A. and Provorse, C. (1996) *The World Almanac of the U.S.A: World Almanac Books*. Mahwah: New Jersey.

[7] Cassel, D. (2000) Virtual vandals, hacktivism takes to the cyberstreets. *Sonoma County Independent* (www.metroactive.com).

[8] Center to Bridge the Digital Divide. (2004) *Ecomonics of Market Failure*. Washington State University (www.cbdd.edu).

[9] Center for Science and Technology in Congress. (2000) *Cyber Security Bill to Amend FOIA* (www.aaas.org).

[10] Charney, S. and Mitchell, D. (2004) Law, investigation and ethics: Federal and state computer crime laws. *Handbook of Information Security Management* (www.cccure.org).

[11] Commission on Intergovernmental Relations by the Subcommittee on Natural Disaster Relief. (1955) *Staff Report on Civil Defense and Urban Vulnerability*. U.S. Government Printing Office (www.eisenhower.utexas.edu).

[12] Computer Security Administration. (2004) *Network Security Policy*. Computing and Networking Services (www.utoronto.ca).

[13] Cordesman, A. (2002) *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland.* Praeger Publishers: Westport.

[14] Daneels, A. and Salter, W. (2000) What is SCADA? The European Organization for Nuclear Research *CERN* (http://public.web.cern.ch/public).

[15] Dean, J. (2002) Protecting the physical and cyber homeland: Systems failure. *Government Executive* (www.itsa.org).

[16] Deputy Assistant Secretary for Defense, Security and Information Operations, Critical Infrastructure Protection Directorate (1998) *The Deparment of Defense Critical Infrastructure Protection (CIP) Plan.* The Department of Defense (www.fas.org).

[17] DIBS USA (2004) *Computer Forensics Definitions and Methodologies.* Next Generation Computer Forensics Online (http://www.dibsusa.com).

[18] DoD Insider Threat Mitigation Team. (2000) *Final Report of the Insider Threat Integrated Process Team.* Department of Defense.

[19] Electronic Privacy Information Center. (2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (www.epic.org).

[20] Emergency Response & Research Institute. (2001) Chinese cyber blitz being faced by United States. *Emergency Netnews* (www.emergency.com).

[21] England, Gordon, Deputy Secretary United States Department of Homeland Security. (2003) *Correspondence to the Director, United States General Accounting Office* (www.gao.gov).

[22] Feynman, R. (2001) Lifecycle security and DITSCAP. *IA Newsletter,* **4 (2)**.

[23] Fisher, D. (2003) Cyber plan's future bleak. *E-Week Enterprise News and Reviews* (www.eweek.com).

[24] Fuji-Keizai USA, Inc. (2002) U.S. Next generation networks 2002. *Research and Market News* (www.researchandmarkets.com).

[25] Garner, B. (1999) *Blacks's Law Dictionary, 7th Edition.* West Group: Minnesota.

[26] Gellman, B. (2002, June 27) Cyber-attacks by Al Qaeda feared, terrorists at threshold of using Internet as tool of bloodshed, experts say. *Washington Post,* Washington.

[27] Gershwin, L. (2001) *Cyber Threat Trends and U.S. Network Security.* Statement for the Record to the Joint Economic Committee (www.cia.gov).

[28] Gordon, M. (2002) *The Iowa Homeland Security Initiative: Envisioning the Future.* Iowa Homeland Security (www.iowahomelandsecurity.org).

[29] Government Electronics and Information Technology Association. (2002) Information assurance and critical infrastructure protection: A Federal perspective. *The IWS Information Warfare Site* (www.iwar.org).

[30] Greenhouse, L. (2001, September 30) The nation: Will the Court reassert national authority? *The New York Times*: New York.

[31] Hamilton, A., Jay, J. and Madison, J. (1788) *Federalist 11.* The Federalist.

[32] Hamilton, A., Jay, J. and Madison, J. (1788) *Federalist 32.* The Federalist.

[33] Harman, J., Congresswoman, 36th Congressional District (2002) Homeland Security Information Sharing Act. *Proceedings and Debates of the 107th Congress Second Session* (www.house.gov).

[34] Hayes, F. (1999) Hacker lessons: Frankly speaking. *Computerworld* (www.computerworld.com).

[35] Howard, J. and Lonstaff, T. (1998) *A Common Language for Computer Security Incidents.* Sandia National Laboratories. New Mexico.

[36] InfraGard Executive Board. (2002) *InfraGard Executive Annual Report to Membership.* Federal Bureau of Investigations (www.infragard.net).

[37] Institute for Security Technology Studies, Investigative Research for Information Assurance Group (IRIA). (2002) *Information and Telecommunications Sector Vulnerabilities and Threats.* Institute for Security Technology Studies at Dartmouth College.

[38] IT Professionals Association. (2004) Outsourcing can lead to economic espionage. *The Economic Times Online* (www.economictimes.com).

[39] Joint Chiefs of Staff, Department of Defense (1996) *Information Warfare 4th Edition.*

[40] Joint Chiefs of Staff, Department of Defense (2000) *Information Assurance Through Defense in Depth.*

[41] Kelly, Malcom. (2000) Establishing a computer emergency response team in a global bank. *CHI Publishing* (http://www.chi-publishing.com).

[42] Kincaid, J. and Cole, R. (2002) Issues of Federalism in Response to Terrorism. *Public Administration Review*, **62 (1)**.

[43] Kincaid, J. (2001) Terrorism at the W.T.C. New York: Response from a federal democracy. *Indian Journal of Federal Studies*, **2 (2)**.

[44] Ladenheim, K. (1999) *History of U.S. Federalism*. George Washington University (www.min.net).

[45] Lenkowsky, L. (2002) *Opening Plenary Remarks, National Conference on Community Volunteering and National Service, Salt Lake City, Utah*. Corporation for National and Community Service (www.cns.gov).

[46] Levinson, M. (2003) Public-sector governance: Dire states. *CIO Magazine* (www.cio.com).

[47] Lieberman, J. (2003) *Senate Committee on Governmental Affairs Examines the Department of Homeland Security's Critical Infrastructure Efforts*. (www.senate.gov).

[48] Litt, R. (1997) *Statement of Robert S. Litt, Deputy Assistant Attorney General: Before the Subcommittee on Social Security Senate Ways and Means Committee*. United States Department of Justice (www. cybercrime.gov).

[49] Locke, P. (2001) Pentagon attack puts Arlington to test. *Public Administration Times*, Virginia, **24 (11)**.

[50] Major Cities Chiefs Association. (2002) Terrorism, the impact on state and local law enforcement. *Intelligence Commanders Conference Report* (www.neiassociates.org).

[51] Miller, F. (2003) *National Conference of Commissioners on Uniform State Laws*. Uniform Law Commissioners (www.nccusl.org).

[52] Moteff, J., Copeland, C. and Fischer, J. (2003) *Critical Infrastructures, What Makes an Infrastructure Critical?* Fischer Resources, Science, and Industry Division (www.fas.org).

[53] National Conference of State Legislators. (2004) *State Budget Update*. (www.ncsl.org).

[54] National Conference of State Legislators. (2004) *State Criminal Codes*. (www.ncsl.org).

[55] National Defense University. (2001) *Threats, Vulnerabilities, the Federal Response*. National Defense University Briefing.

[56] National Security Telecommunications and Information Systems Security 4009. (1997) Definition of information assurance. *The Information Warfare Site* (www.iwar.org).

[57] New Hampshire Office of Information Technology. (2003) *Focus, Mission and Implications on State Government Operational Efficiencies* (www.nh.gov).

[58] Nivola, P. (2002) *Reflections on Homeland Security and American Federalism.* The Brookings Institution Press: Washington.

[59] O'Hanlon, M. (2001) *Protecting the American Homeland.* The Brookings Institution Press: Washington.

[60] O'Hara, C. (2002) Cybercorps to extend to states. *Federal Computer Week* (www.fcw.com).

[61] O'Malley, M. (2003, February 17) Taxing homeland security. *Washington Post*, Washington.

[62] Office of the Governor, State of Oklahoma. (2002) *Governor Keating to Attend National Governors' Association Meeting: Homeland Security to be Top Issue.* Oklahoma State Governors Page (www.governor.state.ok.us).

[63] Oklahoma Department of Career and Technology Education. (2004) *Oklahoma CareerTech: About Us.* (www.okcareertech.org).

[64] Oram, A. (2002) The national strategy to secure cyberspace: A somber cyberassesment. *The American Reporter*, Cambridge: Massachucetts.

[65] Partnership for Critical Infrastructure Security. (2004) *Public Policy White Paper. Working Group 3* (www.pcis.org).

[66] Peerenboom, J. (2001) *Infrastructure interdependencies: Overview of Concepts and Terminology.* Pacific Northwest Economic Region (www.pnwer.org).

[67] Perlman, E. (2004) Techtonic shift: Delaware has reformatted the structure and operation of its technology agency. *Governing.Com* (http://governing.com).

[68] Pfleeger, C. and Pfleeger S. (2003) *Security in Computing 3rd Edition.* Prentice Hall PTR: New Jersey.

[69] Richardson, R. (2003) *CSI/FBI Computer Crime and Security Survey.* Computer Security Institute.

[70] Ridge, T. (2003) Cyber Security is Critical to U.S. Infrastructure. *The United States Mission to the European Union* (www.useu.be).

[71] Riley, J. (2003) *Enlist the States in Protecting the Nation.* RAND: California.

[72] Rinaldi, S. (1994) Beyond the Industrial Web: Economic Synergies and Targeting Methodologies. *Air Univerisity Press* (www.fas.org).

[73] Riordan, R., Zegart A. (2002, July 5) City Hall Goes to War. *New York Times*, New York.

[74] Risk Management Process and Risk Assessment: Critical Infrastructure Task Force. (2000) *The Challenge of CIP Interdependencies, Final Report.*

[75] Robinson, C. (1998) Critical infrastructures: Interlinked and Vulnerable. *Issues in Science and Technology Online* (www.issues.org).

[76] Sarkar, D. (2004) Critical Infrastructure Data Sought. *Federal Computer Week* (www.fcw.com).

[77] Shannon, J. (1997) *Middle-Class Votes Bring a New Balance to U.S. Federalism: The Future of the Public Sector*. The Urban Institute (www.urban.org).

[78] Shanor, C. (2001) *American Constitutional Law Structure and Reconstruction.* West Group.

[79] Stoneburner, A., Goguen, A., and Feringa, A. (2001) Risk management guide for information technology systems. *National Institute of Standards and Technology Publication, 800-30.*

[80] Tanner, R. (2004, February 23) Governors seek input on Guard use. *Associated Press: Tulsa World.*

[81] The Gordian Knot Limited (2003) *The Legend of Gordian Knot, and Why We Chose the Name* (www.gordian.co.uk).

[82] The Internet Society. (2003) *The History of the Internet* (www.isoc.org).

[83] The Oklahoma Department of Civil Emergency Management. (2003) *Murrah Federal Building Bombing 19 April 1995 in Oklahoma City, After Action Report.* (www.odcem.ok.us).

[84] The White House. (2003) *Homeland Security Presidential Directive: HSPD 7.* (www.whitehouse.gov).

[85] The White House. (2003) *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (www.whitehouse.gov).

[86] The White House. (2002) *National Strategy to Secure Cyberspace* (www.whitehouse.gov).

[87] The White House. (2000) *The National Plan for Information Systems Protection - Version 1.0: An Invitation to Dialogue* (www.fas.org).

[88] The White House. (2002) *National Strategy for Homeland Security.* Department of Homeland Security (www.whitehouse.gov).

[89] The White House. (1996) *Our Nation's Critical Infrastructures: Working Definitions*. President's Commission on Critical Infrastructure Protection (PCCIP) (www.inf-sec.com).

[90] Treaster, J. (2002, November 15) House votes to help insure terror losses. *The New York Times*: New York.

[91] Tsymbal, V. (1995) *Deterring Information Warfare: A New Strategic Challenge*. Speech given at the Russian-U.S. Conference on evolving post-cold war national security issues.

[92] United States Conference of Mayors. (2003) *Direct Homeland Security Cost Increases Related to War/High Threat Alert*. The U.S. Conference of Mayors Survey on Cities (www.usmayors.org).

[93] United States Department of Energy, Office of Fossil Fuels. (1999) DOE signs major agreement with Exxon to lease idle pipelines at strategic reserve. *Department of Energy Techline* (http://www.fe.doe.gov).

[94] United States Department of Energy. (2002) Cyber-related critical infrastructure identification and protection measures. *Inspector General Audit Report 0545* (www.fe.doe.gov).

[95] United States Department of Homeland Security, Information Analysis and Infrastructure Protection Directorate. (2003) *Project Matrix* (www.ciao.gov).

[96] United States Department of Homeland Security. (2003) *National Cyber Security Division Press Release* (www.4law.co).

[97] United States Department of Justice. (2002) Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (www.cybercrime.gov).

[98] United States Department of Labor, Bureau of Labor Statistics (2003) *Volunteering in the United States* (www.bls.gov).

[99] United States General Accounting Office. (2003) Information security: Progress made, but challenges remain to protect federal systems and the nation's critical infrastructures. *Testimony before the Subcommittee on Technology, Information Policy* (www.gao.gov).

[100] United States General Accounting Office. (2003) Homeland security: Efforts to improve information sharing need to be strengthened. *Report to the Secretary of Homeland Security* (www.gao.gov).

[101] United States Department of Health and Human Services. (2003) HIPAA Security Guidelines Subpart C to Code of Federal Regulations 45, section 164.

[102] United States National Security Agency. (2003) *NSTISSP No. 11 Revised Fact Sheet National Information Assurance Aquistion Policy*. National Institute of Standards and Technology (http://niap.nist.gov).

[103] Walczak, R., Dunham, S. and Mahnusson, P. (2002) America's biggest job. *Business Week Online* (www.businessweek.com).

[104] Warner, M. (2002) *Regional Homeland Security Summit Brings Together Virginia, Maryland, and D.C.* State of Virginia Regional Press Policy Release (www.commonwealthpreparedness.state.va.us).

[105] Washington File. (2003) U.S. issues national strategy to protect cyberspace. *The IWS Information Warfare Site* (www.iwar.org).

[106] Weiber, L., and Vining A. (1999) *Policy Analysis: Concepts and Practice, 3rd Edition*. Prentice Hall: New Jersey.

[107] Welsh, W. (2001) Cuts in IT programs looming for states. *Washington Technology* (www.washingtontechnoloy.com).

[108] Wilikens, M., and Masera, M. (2002) *Information Infrastructure Interdependencies: Systemic Risk Issues*. 42nd Meeting on Dependable Computing and Fault Tolerance (www.delft2001.tudelft.nl)

[109] Wray, S. (1998) Electronic civil disobedience and the World Wide Web of hacktivism: A mapping of extraparliamentarian direct action net politics. *Proceedings of The World Wide Web and Contemporary Cultural Theory Conference* (http://switch.sjsu.edu).

[110] Yoshihara, C. (2001) *Chinese Information Warfare a Phantom Menace or Emerging Threat?* United States Army Strategic Studies Institute (www.carlisle.army.mil).

[111] Young, E. (2001) *The Balance of Federalism in Unbalanced Times: Should the Supreme Court Reconsider its Federalism Precedents in Light of the War on Terrorism?* FindLaw's Legal Commentary (http://writ.news.findlaw.com).

Supplemental Works not Cited

[112] Alexander, Y. (2002) *Combating Terrorism: Strategies of Ten Countries*. University of Michigan Press: Ann Arbor.

[113] Arquilla, J., and Ronfeldt, D. (2001) *Networks and Netwars*. National Defense Research Institute. RAND: Santa Monica.

[114] Barman, S. (2002) *Writing Information Security Policies*. New Riders Publishing: New York.

[115] Berg, E. (2001) *Technology Forecast, 2001-2003: Mobile Internet: Unleashing the Power of Wireless*. Price Waterhouse Coopers: California.

[116] Boot, M. (2002) *The Savage Wars of Peace: Small Wars and the Rise of American Power.* Persus Books Group. New York.

[117] Carr, C. (2002) *The Lessons of Terror: A History of Warfare Against Civilians.* Random House: New York.

[118] Carter, A. (2001) The architecture of government in the face of terrorism. *International Security*, **26 (3)**.

[119] Cirincione, J. (2002) *Repairing the Regime: Preventing the Spread of Weapons of Mass Destruction.* Routledge: New York.

[120] Cordesman, A. (2002) *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland.* Praeger: Connecticut.

[121] Cronin, I. (2002) *Confronting Fear: A History of Terrorism.* Thunder's Mouth Press: New York.

[122] Douhet, G. (1942) *Command of the Air*. Office of Air Force History.

[123] Espositio, J. (1999) *The Islamic Threat: Myth or Reality, 3rd Edition.* Oxford University Press: New York.

[124] Federal Bureau of Investigation. (2003) *Most wanted terrorists: Khalid Shaikh Mohammed* (www.fbi.gov).

[125] Ford, F. (2001) *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, 2nd Edition.* Prentice-Hall PTR: New Jersey.

[126] Garfinkel, S. (2002) *Web Security, Privacy and Commerce, 2nd Edition.* O'Reilly: California.

[127] Hewitt, C. (2003) *Understanding Terrorism in America: From the Klan to Al Qaeda.* Routledge: London.

[128] Hobijn, B. (2002) What will homeland security cost? *Federal Reserve Bank of New York Policy Review* (www.newyorkfed.org).

[129] Hoffman, B. (1998) *Inside Terrorism.* Columbia University Press: New York.

[130] Homer-Dixon, T. (2002) *The Ingenuity Gap.* Vintage Books: New York.

[131] Homer-Dixon, T. (1999) *Environment, Scarcity, and Violence.* Princeton University Press: New Jersey.

[132] Huntington, S. (1997) *The Clash of Civilizations and the Remaking of World Order*. Touchstone: New York.

[133] Johnson, C. (2000) *Blowback: The Costs and Consequences of American Empire*. Henry Holt and Company: New York.

[134] Karsh, E. (2001) *Empires of the Sand: The Struggle for Mastery in the Middle East 1789-1923*. Harvard University Press: Massachusetts.

[135] Kramer, J. (2002) *Lone Patriot: The Short Career of an American Militiaman.* Pantheon Books: New York.

[136] Kushner, H. (1998) *The Future of Terrorism: Violence in the New Millennium.* Sage Publications: California.

[137] Laqueur, W. (1999) *The New Terrorism: Fanaticism and the Arms of Mass Destruction.* Oxford University Press: New York.

[138] Lesser, I. (1999) *Countering Terrorism: The New Terrorism*. RAND: California.

[139] Lessig, L. (2002) *The future of ideas: The Fate of the Commons in a Connected World*. Random House: New York.

[140] Lewis, B. (2002) *What Went Wrong? Western Impact and Middle Eastern Response*. Oxford University Press: New York.

[141] Maney, K. and McMahon, P. (2000) Love bug created in ordinary petri dish. *USA Today* (www.usatoday.com).

[142] Mason, A. (2002) A crime by any other name. *Freedom Magazine* (www.theta.com).

[143] Oates, P. (2002) Supporting the national strategy for homeland security: The role of the National Guard. *Harvard Perspectives on Preparedness*, **8 (1)**.

[144] Oklahoma Department of Public Safety. (2002) *Oklahoma State Senate Legislative Brief* (www.lsb.state.ok.us).

[145] OneNet Oklahoma. (2003) Oklahoma's telecommunications network business plan. *OneNet* (www.onenet.net).

[146] Oren, M. (2002) *Six Days of War: June 1967 and the Making of the Modern Middle East*. Oxford University Press: New York.

[147] Pasanen, Y. (2003) The implications of virtual deception. *Air and Space Power Chronicles* (www.airpower.maxwell.af.mil).

[148] Pillar, P. (2001) *Terrorism and U.S. Foreign Policy*. Brookings Institution Press: Washington.

[149] Pipkin, D. (2000) *Information Security: Protecting the Global Enterprise.* Prentice Hall PTR: New Jersey.

[150] Posse Comitatus Act. (2002) *U.S. Posse Comitatus 18 USC 1385.* LexisNexis (www.lexis.com).

[151] Priest, D. (2002) *The Mission: Waging War and Keeping Peace with America's Military.* W.W. Norton and Company: New York.

[152] Printz v. United States. (2002) *Printz v. United States, 521 U.S. 898.* LexisNexis (www.lexis.com).

[153] Public Broadcasting Service. (2003) *History of Advanced Research Project Agency.* (www.pbs.org).

[154] Radin, M. (2002) *Internet Commerce: The Emerging Legal Framework.* Foundation Press: New York.

[155] Schick, A. (2001) *The Federal Budget: Politics, Policy, Process.* Brookings Institution Press: Washington.

[156] Sofaer, A. (2000) *A Proposal for an International Convention on Cybercrime and Terrorism.* Center for International Security and Cooperation: Stanford University, California.

[157] The U.S. Conference of Mayors (2002) *The Cost of Heightened Security in America's Cities: A 192-city survey.* The U.S. conference of Mayors Survey On Cities (www.usmayors.org).

[158] The White House. (2002) *Remarks by the President on Homeland Security and the Budget.* Presidential Speech on homeland and economic security at Mt. Rushmore (www.whitehouse.gov).

[159] Tipton, H. (2000) *Information Security Management Handbook, 4th Edition.* Auerbach: New York.

[160] Weimer, D. (1989) *Policy Analysis: Concepts and Practice, 3rd Edition.* Prentice Hall: New Jersey.